Physical Security Criteria for Federal Facilities

An Interagency Security Committee Standard

April 12, 2010

For Official Use Only (FOUO)

Cover Photo: This is a photograph of the U.S. Nuclear Regulatory Commission (NRC) Headquarters facilities in Rockville, MD. This complex represents the broad applicability and scope of this document. The Headquarters facility, located at the NRC White Flint North Complex, includes both a Government-owned building and a Government-leased building with the incorporation of aesthetic security measures at the complex.

The NRC One White Flint North building (left) is Government-owned. The General Services Administration (GSA) purchased it from the private sector in 1986 on behalf of the NRC. GSA leases the NRC Two White Flint North building (right) on behalf of the NRC. Combined, these two buildings provide approximately 576,000 usable square feet of space for NRC operations.

Photo courtesy of the NRC.

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with Department of Homeland Security (DHS) policy relating to FOUO information and is not to be released to the public or personnel who do not have a valid "need-to-know" without prior approval of the authorized DHS official.

At a minimum, this document will be disseminated only on a need-to-know basis, and when unattended, will be stored in a locked container or area offering sufficient protection against theft, compromise, inadvertent access and unauthorized disclosure.

When no longer needed, destroy this material by shredding, pulping, or burning to assure destruction beyond recognition.

This Page Intentionally Left Blank

Preface

Todd M. Keil
Assistant Secretary for Infrastructure Protection

Protecting Federal employees and the public who visit U.S. government-owned or leased facilities from all hazards is a complex and challenging responsibility. It is also one of our top national priorities and the mission of the Interagency Security Committee (ISC).

As Chair of the ISC, I am pleased to introduce a new interim ISC standard, *Physical Security Criteria for Federal Facilities*, which is to be used during a 24-month validation period. This validation period will allow for user input to inform the final standard.

This standard establishes a baseline set of physical security measures to be applied to all Federal facilities based on their designated facility security level. It also provides a framework for the customization of security measures to address unique risks faced at each facility.

The one-standard approach applied in this document offers several advantages to the Federal security community. It provides an integrated, single source of physical security standards for all Federal facilities; opportunity and guidance for flexibility and customization of these standards; and integration of new standards and concepts contained in two other key ISC documents being issued this year: *Design-Basis Threat: An ISC Report;* and *Facility Security Committees: An Interagency Security Guideline.*

This Standard supersedes the physical security standards in the *ISC Security Standards for Leased Space, ISC Design Criteria for New Federal Office Buildings and Major Modernization Projects*, and the *1995 DOJ Report.*

The new Standard is applicable to all buildings and facilities in the United States occupied by Federal employees for nonmilitary activities. These include existing buildings, new construction, or major modernizations; facilities owned, to be purchased, or leased; stand-alone facilities, Federal campuses, and where appropriate, individual facilities on Federal campuses; and special-use facilities.

Any facility entering the inventory on or after the date of issuance (April 12, 2010) shall use the physical security criteria (PSC) process in accordance with this Standard. All Federal Facilities that were in the inventory prior to April 12th must use the PSC process on their next scheduled assessment.

This Standard is a significant milestone, representing exemplary collaboration across the entire ISC. I want to especially commend members of the PSC working group for all the hard work they put into the development of the Standard.

Todd M. Keil
Assistant Secretary for Infrastructure Protection

This Page Intentionally Left Blank

Contents

Figures

1.0 Background

The "Vulnerability Assessment of Federal Facilities" issued by the U.S. Department of Justice in 1995 (1995 Report) established the first set of Government-wide physical security standards for Federal facilities. Over the ensuing years, the Interagency Security Committee (ISC) issued additional security standards for buildings to be constructed or undergoing major modernization, and for lease acquisitions.

In light of the increased threat made apparent by the terrorist attacks of September 11, 2001, and the prevailing Homeland Security Alert Condition being "Yellow/Elevated," the ISC membership decided in 2006 to update, expand and, where necessary, clarify all security standards for protecting Federal facilities. Working groups were established by the ISC to update and coordinate the revisions of all facility security standards and publish them in one "compendium."

The first product of the working groups, "Facility Security Level Determination for Federal Facilities," was issued on March 10, 2008. It applies to all facilities whether they are Government-owned or leased, to be constructed, modernized, or purchased. The facility security level (FSL) determination document became the foundation for all future ISC security standards.

As the ISC working groups progressed, they concluded that one approach in applying security standards should be followed. Further, the groups recognized that security requirements should not be driven by the type of space occupied, but by the security needs of the Federal tenant(s) occupying the space. The groups readily agreed on an underlying unifying principle – regardless of the type of building, the nature of the Government's occupancy (owned or leased), or whether the building exists in concrete and steel or only on paper, the risks that face the facility itself, the agency mission, and the personnel occupying the facility should be mitigated to an acceptable level. Accordingly, the ISC membership concluded that one ISC standard should govern all facility physical security requirements and ensure that security becomes an integral part of the operations, planning, design, construction/renovation, or acquisition of Federal facilities. Specifically, the FSL directs the user to a set of baseline standards which may be customized to address site-specific conditions.

Regardless of the type of building, the nature of the government's occupancy (owned or leased), or whether it exists in concrete and steel or only on paper, the risks that face the facility itself, the agency mission, and the personnel occupying the facility should be mitigated to an acceptable level.

2.0 Applicability and Scope

"Physical Security Criteria for Federal Facilities—An Interagency Security Committee Standard" (the Standard) establishes a baseline set of physical security measures to be applied to all Federal facilities at each FSL – I, II, III, IV, and V. Further, this Standard provides a framework for the customization of security measures to address unique risks faced at each facility. This Standard is issued pursuant to the authority of the ISC contained in Executive Order 12977, October 19, 1995, "Interagency Security Committee," as amended by Executive Order 13286, March 5, 2003. Each executive agency and department shall comply with the policies and recommendations in this Standard, except where the Director of Central Intelligence determines that compliance would jeopardize sources and methods.

The threats addressed by this Standard are primarily man made. Other threats to buildings, such as earthquakes, floods, fire, or wind storms are beyond the scope of this document and addressed in applicable construction standards.

This Standard is applicable to all buildings and facilities in the United States occupied by Federal employees for nonmilitary activities. These include existing buildings, new construction, or major modernizations; facilities owned, to be purchased, or leased; stand-alone facilities, Federal campuses, and where appropriate, individual facilities on Federal campuses; and special-use facilities.

The threats addressed by this Standard are primarily man made. Other threats to buildings, such as earthquakes, fire, or storms are beyond the scope of this document and are addressed in applicable construction standards, although many of the countermeasures identified will contribute to mitigating natural hazards. Further, this document assumes that security managers will implement countermeasures in full compliance with applicable sections of the United States Code (U.S.C.), Code of Federal Regulations (CFR), Federal Management Regulations, Americans with Disabilities Act requirements, Occupational Safety and Health Administration regulations, Fire and Life Safety codes, and all applicable Executive Orders and Presidential Directives.

The security decision process is a piece of an overall facility management or real estate acquisition process.

This Standard defines a process for determining the security measures required at a facility. It is critical that departments and agencies recognize that the security decision process is an integral part of an overall facility management process and real estate acquisition process. It must be fully integrated to be the most effective.

This Standard supersedes the physical security standards in the "ISC Security Standards for Leased Space," "ISC Design Criteria for New Federal Office Buildings and Major Modernization Projects," both dated September 29, 2004, and the 1995 Report.

In order to keep pace with the changing nature of the threat to Federal facilities, updates to this Standard will be made periodically. Users of this document should visit the ISC Web site (www.dhs.gov/isc) for relevant information that may affect this Standard and other ISC documents related to the security of Federal facilities.

3.0 Document Control

This document is For Official Use Only (FOUO) and should be released only to those with a need-to-know. In the past it has been common practice to provide design consultants or realty brokerage firms with a complete copy of a standards document. This practice provides them more information than required to complete their work.

This document is not to be released in its entirety to design consultants. Specific security requirements based on this Standard are to be developed by the government and provided to design consultants.

Government representatives should develop specific security requirements—expressed in performance terms where possible—and provide them to design consultants. In this manner, only the minimum required information will be released outside of the Government, and information that is outside the scope of a project will not be released to persons without a valid need-to-know.

All risk assessments, specific security requirements, and design documents developed in accordance with this Standard must be marked as FOUO or higher, as appropriate, protected accordingly, and should be retained by the decision-makers in the risk management process.

4.0 Definitions

For the purposes of this Standard, the following definitions apply. For ease of comparison, the definitions are grouped and listed according to their relationship to each other. Appendix B provides an alphabetized list of acronyms and definitions.

4.1 General Definitions

Facility Security Level (FSL): A categorization based on the analysis of several security-related facility factors, which serves as the basis for the implementation of physical security measures specified in ISC standards.

Level of Protection (LOP): The degree of security provided by a particular countermeasure or set of countermeasures. Levels of protection used in this Standard are Minimum, Low, Moderate, High, and Very High.

Baseline LOP: The degree of security provided by the set of countermeasures identified in this document for each FSL which must be implemented unless a deviation (up or down) is justified by a risk assessment.

Necessary LOP: The degree of security determined to be needed to mitigate the assessed risks at the facility.

Existing LOP: The degree of security provided by the set of countermeasures determined to be in existence at a facility.

Customized LOP: The final set of countermeasures developed as the result of the risk-based analytical process.

Risk: A measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence.

Level of Risk: The combined measure of the threat, vulnerability, and consequences posed to a facility from a specified undesirable event.

Undesirable Event: An incident that has an adverse impact on the facility occupants or visitors, operation of the facility, or mission of the agency.

Threat: The intention and capability of an adversary to initiate an undesirable event.

Design-Basis Threat (DBT): A profile of the type, composition, and capabilities of an adversary.

Vulnerability: A weakness in the design or operation of a facility that an adversary can exploit.

Consequence: The level, duration, and nature of the loss resulting from an undesirable event.

Risk Assessment: The process of evaluating credible threats, identifying vulnerabilities, and assessing consequences.

Risk Mitigation: The application of strategies and countermeasures to reduce the threat of, vulnerability to, and/or consequences from an undesirable event.

Risk Management: A comprehensive approach to allocating resources for the protection of a facility, assets, and occupants to achieve an acceptable level of risk. Risk management decisions are based on the application of risk assessment, risk mitigation, and—when necessary—risk acceptance.

Risk Acceptance: The explicit or implicit decision not to take an action that would affect all or part of a particular risk

Risk Assessment Report: The documentation of the risk assessment process to include the identification of undesirable events, consequences, and vulnerabilities, and the recommendation of specific security measures commensurate with the level of risk.

4.2 Locations

Building: An enclosed structure (above or below grade).

Facility: Space built or established to serve a particular purpose. The facility is inclusive of a building or suite and associated support infrastructure (e.g., parking or utilities) and land.

Federal Facilities: Government-leased and -owned facilities in the United States (inclusive of its territories) occupied by executive branch Federal employees for nonmilitary activities.

Setback: The distance from the façade to any point where an unscreened or otherwise unauthorized vehicle can travel or park.

Standoff: Distance between an explosive device and its target.

Site: The physical land area controlled by the Government by right of ownership, leasehold interest, permit, or other legal conveyance, upon which a facility is placed (Figure 1).

Site Perimeter: The outermost boundary of a site. The site perimeter is often delineated by the property line (Figure 1).

Campus: Two or more Federal facilities located on one site and typically sharing some aspects of the environment, such as parking, courtyards, private vehicle access roads, or gates and entrances to connected buildings. A campus also may be referred to as a "Federal center" or "complex."

Site Entry: A vehicle or pedestrian access point into, or exit from, the site (Figure 1).

Adjacency: A building or other improvement that abuts or is proximate to a multiple building site, a specific building within a multiple building site, or a single building site (Figure 1).

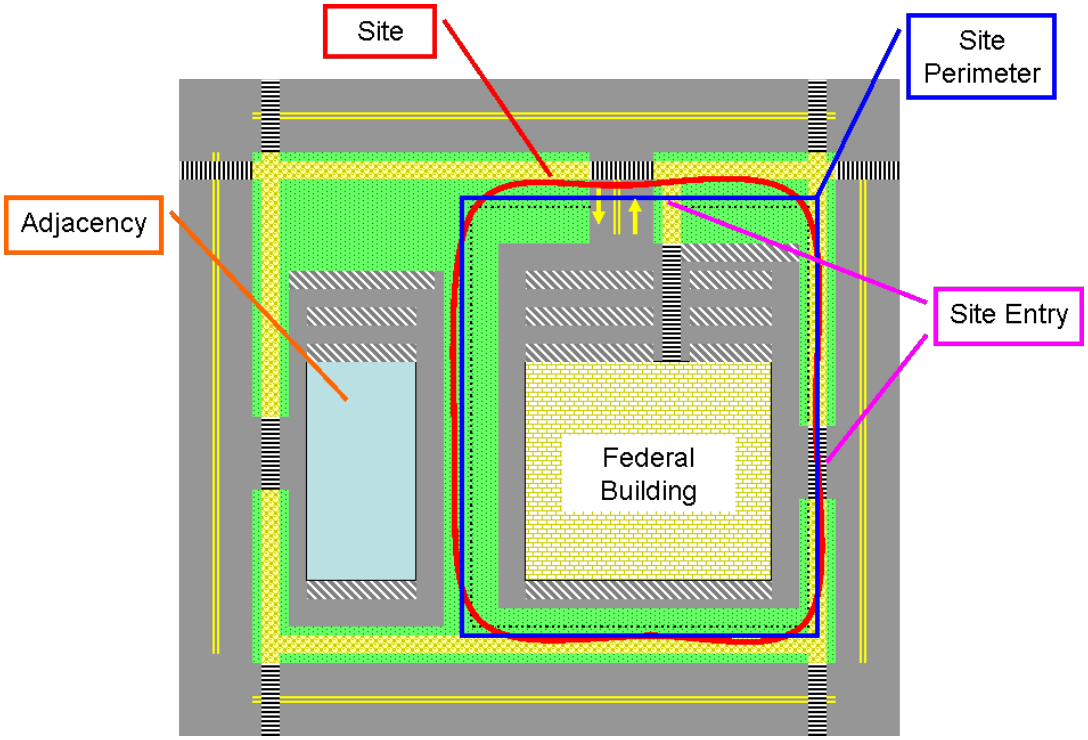


Figure 1. Site Reference Diagram

Building Envelope: The outside surface and dimensions of a building, inclusive of the façade and roof (Figure 2).

Façade: The exterior face of a building, inclusive of the outer walls and windows (Figure 2).

Building Entry: An access point into, or exit from, the building (Figure 2).

Exterior: Area between the building envelope and the site perimeter (Figure 2).

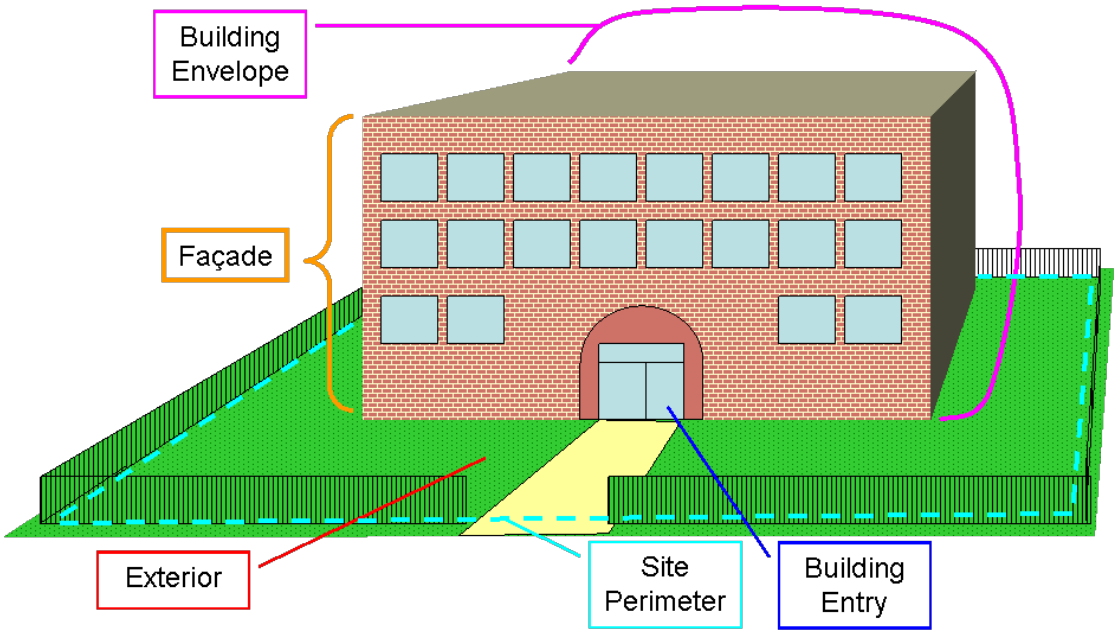


Figure 2. Building Reference Diagram

Suite: One or more contiguous rooms occupied as a unit (Figure 3).

Suite Perimeter: The outer walls encircling a suite (Figure 3).

Suite Entry: An access point into, or exit from, the suite (Figure 3).

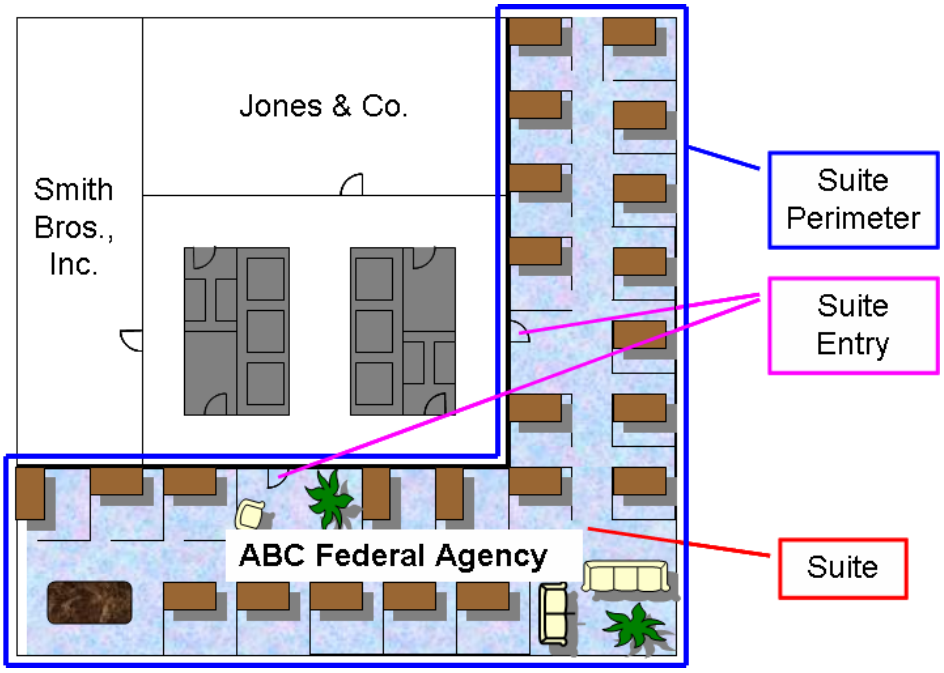


Figure 3. Suite Reference Diagram

Interior: Space inside a building controlled or occupied by the Government.

Critical Areas: Areas that if damaged and/or compromised could have significant adverse consequences for the facility occupants or visitors, operation of the facility, or mission of the agency. Also may be referred to as "limited access areas," "restricted areas," or "exclusionary zones." Critical areas do not necessarily have to be within Government-controlled space (e.g., generators located outside Government-controlled space).

4.3 Organizations and Entities

Federal Departments and Agencies: Those executive departments enumerated in 5 U.S.C. 101 and DHS, independent establishments as defined by 5 U.S.C. 104(1), Government corporations as defined by 5 U.S.C. 103(1), and the U.S. Postal Service.

Designated Official (DO): The highest ranking official of the primary tenant agency of a Federal facility or, alternatively, a designee selected by mutual agreement of tenant agency officials.

Primary Tenant: The Federal tenant identified by Bureau Code in OMB Circular No. A-11, Appendix C, which occupies the largest amount of rentable space in a federal facility.

Facility Security Committee (FSC): A committee responsible for addressing facility-specific security issues and approving the implementation of security measures and practices. The FSC consists of representatives of all Federal tenants in the facility, the security organization, and the owning or leasing department or agency. In the case of new construction, major modernization, alternation, or lease actions, the FSC also will include the construction or lease procurement project team and the planned tenant(s). The FSC was formerly known as the Building Security Committee (BSC).

Security Organization: The Government agency or an internal agency component responsible for physical security for the specific facility.

Occupant: Any person who is permanently or regularly assigned to the facility and displays the required identification badge/pass for access. The FSC establishes the thresholds for determining who qualifies for "occupant" status.

Visitor: Any person entering the government facility who does not possess the required identification badge/pass for access or who otherwise does not qualify as an "occupant."

4.4 Acquisition and Occupancy

New Construction: A project in which an entirely new facility is to be built.

Existing Federal Facility: A facility that has already been constructed or for which the design and construction effort has reached a stage where design changes may be cost prohibitive.

Major Modernization: The comprehensive replacement or restoration of, or addition to, virtually all major systems, tenant-related interior work (such as ceilings, partitions, doors, floor finishes, etc.), or building elements and features.

Alteration: A limited construction project for an existing building that comprises the modification or replacement of one or a number of existing building systems or components. An alteration goes beyond normal maintenance activities but is less extensive than a major modernization.

Lease Construction (Build-to-Suit): A new construction project undertaken by a lessor in response to a specific requirement for the construction of a new facility for the Government.

Lease Extension: An extension of the expiration date of a lease to provide for continued occupancy on a short-term basis.

Lease Renewal (Exercised Option): The exercising of an option to continue occupancy based upon specified terms and conditions in the current lease agreement.

New Lease: A lease established in a new location when space must be added to the current leased space inventory.

Succeeding Lease: A lease established when the Government seeks continued occupancy in the same space at the same leased location, whose effective date immediately follows the expiration date of the existing lease.

Superseding lease: A lease that replaces an existing lease, prior to the scheduled expiration of the existing lease term.

Outlease: The practice of an owning Government agency leasing Government space to nongovernmental tenants.

Government-Owned: A facility owned by the United States and under the custody and control of a Federal department or agency.

Special-Use Facilities: An entire facility or space within a facility itself that contains environments, equipment, or data normally not housed in typical office, storage, or public access facilities. Examples of special-use facilities include, but are not limited to, high-security laboratories, hospitals, aircraft and spacecraft hangers, or unique storage facilities designed specifically for such things as chemicals and explosives.

5.0 Decision-making

Security organizations are responsible for identifying and analyzing threats and vulnerabilities, and recommending appropriate countermeasures. The decision to implement those recommendations and mitigate the risk, or to accept risk, is that of the Facility Security Committee (FSC). Together, the FSC and the security organization are responsible for identifying and implementing the most cost-effective countermeasure appropriate for mitigating a vulnerability, thereby, reducing the risk to an acceptable level. The FSC thus plays a critical role in the decision-making process.

The decision as to whether fully mitigate or accept risk is that of the building tenants. The tenants must either pay for the recommended security measures and reduce the risk, or accept the risk and live with the potential consequences.

To make an informed risk-based decision regarding the mitigation or the acceptance of risk, collaboration between the security organization and the decision-making authority is required. For any countermeasure that is recommended, the security organization must provide all information pertinent to the decision—the nature of the threat, the specific vulnerabilities that must be addressed, a complete understanding of the potential consequences, and the costs. The FSC has the need-to-know this information in order to make a decision.

The FSC members must have the authority, appropriate security clearance, and access to expert resources (e.g., security, facility, and finance) to gain a sufficient understanding of the relevant issues so as to render a sound decision. This does not mean only an understanding of the security issues, but also of the mission and priorities of those who occupy (or will occupy) the building and of the agency as a whole, and the associated cost implications.

The security organization must provide all information pertinent to the decision – the nature of the threat, specificity on the vulnerabilities that must be addressed, complete understanding of the potential consequences, and costs.

Once a credible and documented risk assessment has been presented to and accepted by the decision maker(s), the security provider is not liable for any future decision to accept risk. This does not exempt the security provider from their liability associated with the accuracy and completeness of the risk assessment itself or from implementation of countermeasures.

Decisions made pursuant to this process must be thoroughly documented, from FSL determination and analysis of the LOP, to the implementation of (or decision not to implement) countermeasures.

For further information on the role and responsibilities of the FSC, refer to the ISC standard for Facility Security Committees.

6.0 How To Apply This Standard

Once an FSL has been determined, departments and agencies will either implement the complete set of baseline security measures applicable to the security level of the particular facility, or customize those security measures as necessary to achieve an acceptable level of protection.

The application of this Standard shall follow the analytical process outlined in Section 6.1, regardless of the type of project or occupancy involved. The complexity of the project will determine the level of effort needed to apply this Standard to a specific facility.

Section 6.2 addresses how the type of occupancy impacts the application of this process and how countermeasure recommendations resulting from the process are to be implemented.

6.1 General

The application of this Standard is predicated on an FSL designation using the ISC's Standard, "Facility Security Level Determinations for Federal Facilities." Once an FSL has been determined, departments and agencies will use the following decision-making process resulting in either:

- The application of the baseline LOP applicable to the facility's FSL; or,
- The application of a customized LOP to address facility-specific conditions.

The objective of the defined risk management process is to identify an achievable level of protection that is commensurate with – or as close as possible to – the level of risk, without exceeding the level of risk.

Application of this Standard ensures a comprehensive approach to meeting Federal facility security needs in today's threat environment, and that the scope (and cost) of security is commensurate with the risk posed to a facility. Figure 4, Risk Management Process, on the following page depicts the steps required to apply this Standard and identifies the sections (6.1.1 through 6.1.13) that explain each step. The objective of this risk management process is to identify an achievable LOP that is commensurate with—or as close as possible to—the level of risk, without exceeding the level of risk.

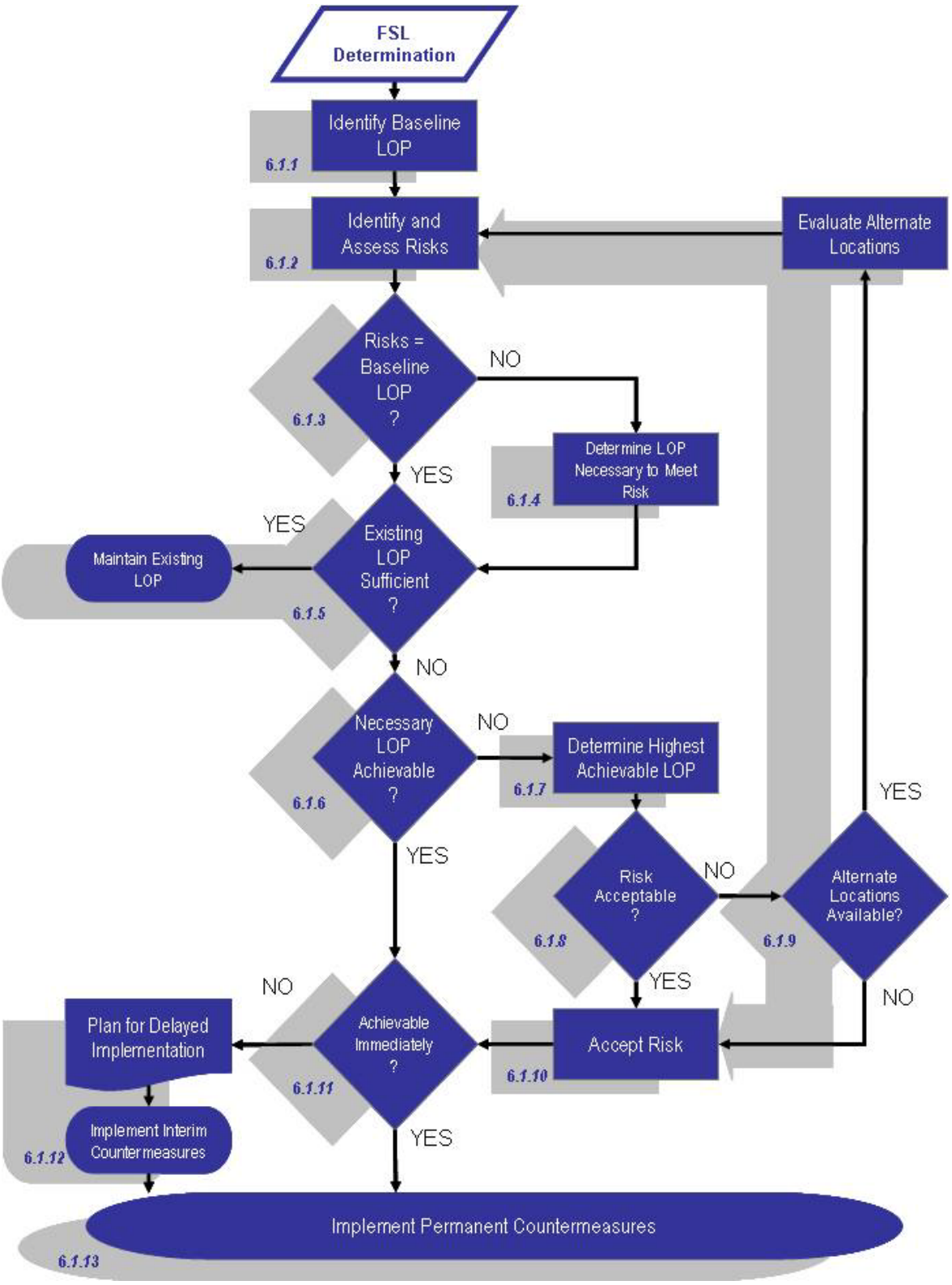


Figure 4. Risk Management Process

6.1.1 Identify Baseline Level of Protection

Each FSL corresponds directly to a LOP and associated set of baseline security measures.

Each FSL corresponds to a level of risk, which then relates directly to an LOP and associated set of baseline security measures. Comparatively speaking, Level I facilities face a minimum level of risk, and thus the baseline LOP for a Level I facility is "Minimum;" Level II corresponds to Low; Level III to Medium; Level IV to High; and Level V to Very High (Figure 5).

Facility Security Level	Level of Risk	Baseline Level of Protection
I	Minimum	Minimum
II	Low	Low
III	Medium	Medium
IV	High	High
V	Very High	Very High

Figure 5. Relationship between FSL, Risk, and LOP

Section 7.0, "Security Criteria," contains tables that list security measures. Each table includes columns of countermeasures aligned to each LOP. All countermeasures in the column applicable to an FSL make up the baseline LOP for a facility (Figure 6).

Security Criterion	Level I - Minimum	Level II - Low	Level III - Medium	Level IV - High	Level V - Very High
Space Planning	No special measures required.	No special measures required.	Locate critical systems and areas at least 25 feet away from loading docks, entrances, and uncontrolled parking, or implement standoff, hardening and venting methods to protect critical areas from the DBT at these locations.	Locate critical systems and areas at least 25 feet away from loading docks, entrances, and uncontrolled parking, or implement standoff, hardening and venting methods to protect critical areas from the DBT at these locations.	Implement standoff, hardening and venting methods to protect critical areas from the DBT at loading docks, entrances, and uncontrolled parking.
Access to Non-public Areas	Use signage to designate non-public areas and establish procedures to prevent unauthorized access.	Use signage to designate non-public areas and establish procedures to prevent unauthorized access.	Use signage, stanchions, counters, furniture, knee walls, etc., to establish physical boundaries to control access to non-public areas.	Use signage, walls, electronic access co and/or security guar establish physical boundaries to contro access to non-public	
Security of Critical Areas	Lock doors to critical areas and establish procedures to limit access into critical areas to authorized personnel only.	Lock doors to critical areas and establish procedures to limit access into critical areas to authorized personnel only.	Install electronic access control and IDS to control and monitor access into critical areas.	nstall electronic acc control and IDS to c and monitor access critical areas.	

Criteria in this column comprise the baseline LOP for Level III facilities

Figure 6. Sample Criteria Table

By determining which countermeasures are applicable to the FSL, a baseline LOP is identified (Figure 7). Continue to step 6.1.2.

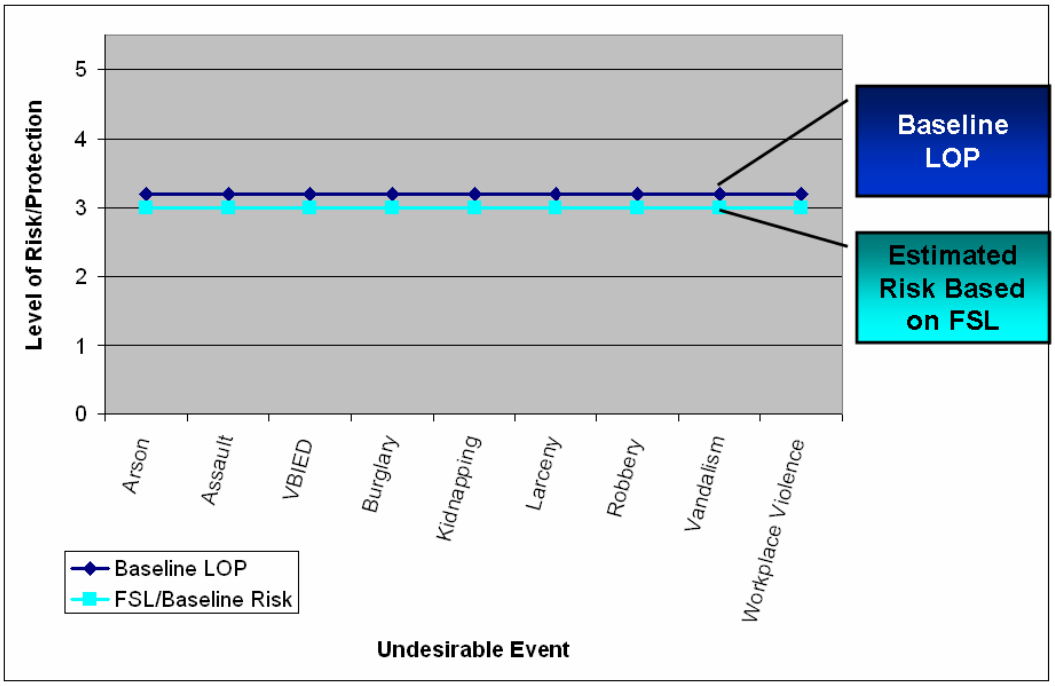


Figure 7. Baseline of Risk, Mitigated by a Baseline LOP

6.1.2 Identify and Assess Risks

To determine if the baseline LOP is sufficient or if customization is needed, the risks to a facility must first be identified and assessed.

The tables in Section 7.0 provide a broad range of undesirable events that may impact Federal facilities. Regardless of the level of effort involved in the identification and assessment of risk, the analysis must consider all of these undesirable events. In assessing actual risks at the facility, the variance of the risk from the baseline is identified (Figure 8).

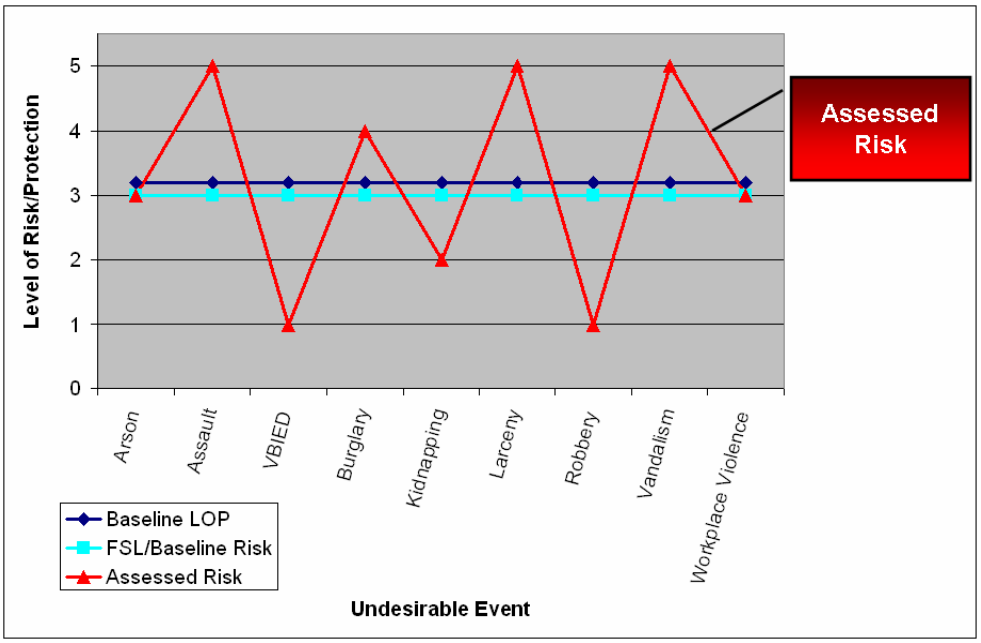


Figure 8. Assessed Risk

Risk is a function of the values of threat, consequence, and vulnerability. The objective of risk management is to create a level of protection that mitigates vulnerabilities to threats and their potential consequences, thereby reducing risk to an acceptable level. Ideally, all risk would be eliminated; practically this is not feasible.

There are a variety of mathematical models available to calculate risk and to illustrate the impact of increasing protective measures on the risk equation. For the purposes of this Standard, the assumption is made at this step of the process that there are no countermeasures in place and complete vulnerability exists. In a new construction project, that is the case; for existing buildings, the existing LOP — and the remaining actual vulnerability — will be assessed in Step 6.1.5. This approach is necessary to ensure that all security criteria will be considered as the process is

completed, and to define the relationship between the level of risk and the LOPs as illustrated in 6.1.1. The level of risk must be mitigated by a commensurate LOP. For example, a high level of risk must be mitigated by implementing a high LOP.

The assessment of risk in this step does not necessarily entail a comprehensive on-site risk assessment. For existing facilities, site visits are beneficial. For new construction or a new lease, no facility may yet exist, and thus the assessment would be based on a conceptual design or set of requirements.

This Standard does not mandate the use of a specific risk assessment methodology. The methodology, software tools, training, and personnel requirements may be unique to the agency. The methodology chosen should adhere to the fundamental principles of a sound risk assessment methodology.

- The methodology must be credible, and assess the threat, consequences, and vulnerability to specific acts.
- The methodology must be reproducible, and produce similar or identical results when applied by various security professionals.
- The methodology must be defensible, and provide sufficient justification for deviation from the baseline.

In practice, various methodologies provide varying outputs, from numbers and percentages to qualitative ratings such as "low" or "green." Each department or agency must determine what outputs from their respective methodologies correlate with each enumerated LOP.

In a multitenant facility where multiple risk assessments may be conducted by different security organizations, the FSC will need to evaluate the outputs and determine what countermeasure recommendations to implement, or if a single risk assessment will be accepted for application.

Once risks have been identified and assessed, continue to step 6.1.3.

Levels of risk determined for each undesirable event should be mitigated by countermeasures that provide a commensurate LOP — the higher the risk, the higher the LOP. Unless deviation is justified by a documented risk assessment, the baseline LOP must be implemented.

6.1.3 Decision Point: Are Risks Adequately Addressed by the Baseline LOP?

Levels of risk determined for each undesirable event should be mitigated by countermeasures that provide a commensurate LOP—the higher the risk, the higher the LOP. The FSL determination is an estimation of the level of risk at a facility. The baseline LOP is intended to mitigate that estimated risk.

The security organization should determine whether the countermeasures

contained in the baseline LOP adequately mitigate known or anticipated risks to the facility. The baseline LOP may be too high (more stringent than necessary) or too low (leaving a vulnerability unmitigated), compared to the level of risk.

If, in assessing the risks to various undesirable events, it is determined that the actual risks faced by the facility are predominantly higher or lower than the FSL, the FSL determination should be re-examined.

⇧ If the baseline LOP adequately addresses the risk(s), plan to implement all of the baseline countermeasures for the LOP. Go to step 6.1.5.

- Or –

If the baseline LOP does not appropriately address the risk(s) (is too high or too low), the necessary LOP must be determined. Continue to step 6.1.4.

If, in assessing the risks of various undesirable events, it is determined that the actual risks faced by the facility are predominantly higher or lower than the FSL, the FSL determination should be re-examined.

6.1.4 Determine the LOP Necessary to Adequately Mitigate Risk(s)

Variations in the nature of mission, location, and physical configuration of a facility may create unique risks or risks that are relatively higher or lower in some cases than at other facilities with the same FSL. The baseline LOP may not address those risks appropriately. It may provide too little protection (e.g., the baseline LOP is medium, but the assessed risk to larceny is very high), leaving an unmitigated risk. Or, it may provide more protection than is necessary (e.g., the baseline LOP is medium, but the assessed risk to armed robbery is very low), resulting in the expenditure of resources where they are not needed. This might reduce the availability of resources that could be applied elsewhere (Figure 9).

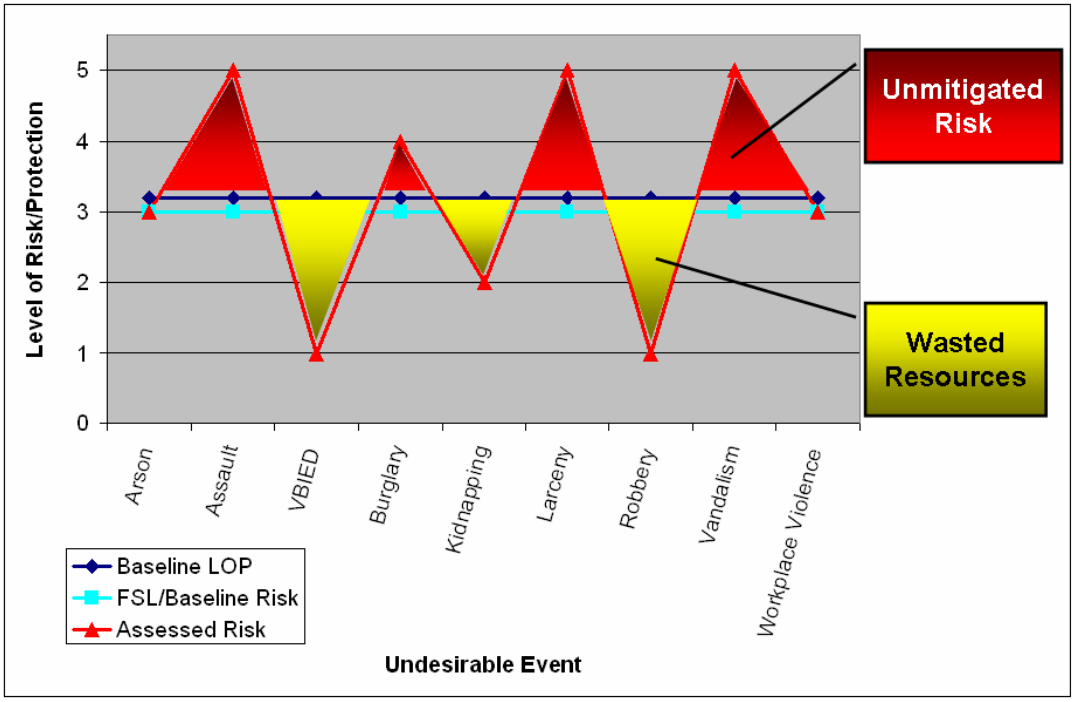


Figure 9. Unmitigated Risk and Wasted Resources

However, by determining the necessary LOP according to a risk assessment, it is possible to ensure that the most cost-effective security program is implemented without waste or lingering vulnerability (Figure 10).

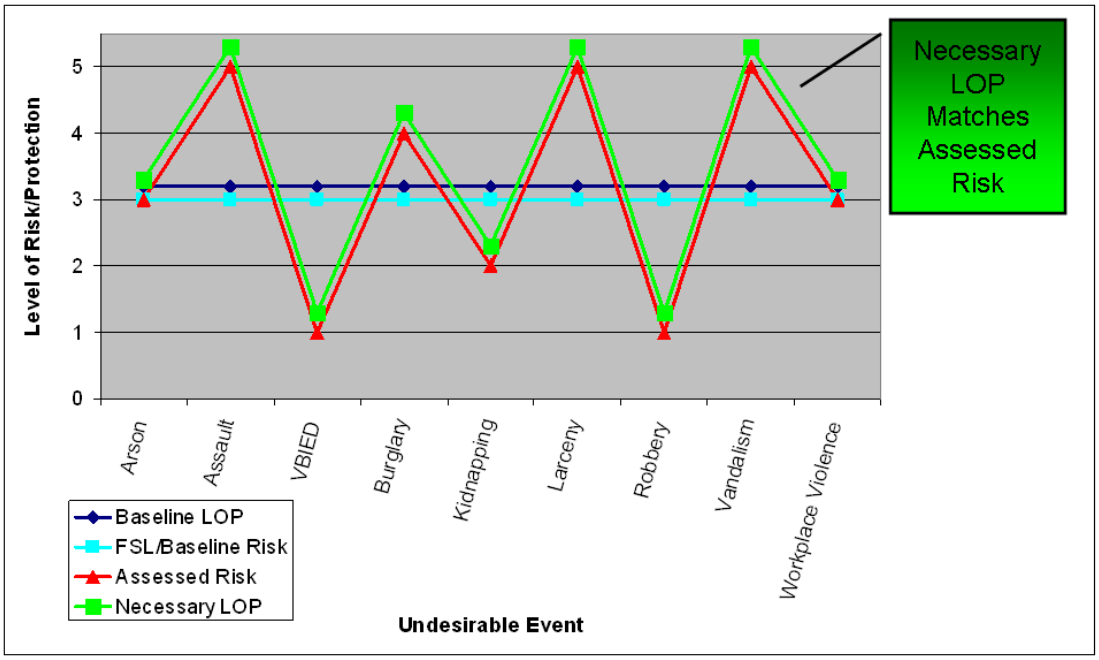


Figure 10. Necessary LOP Matches Assessed Risk

The tables in Section 7.0 will guide the security organization to the countermeasures that are generally considered to mitigate the risk from a particular undesirable event. The matrix identifies a generic set of undesirable events that may impact Federal facilities, and relates them to the applicable security measures. A brief explanation of each undesirable event can be found starting on page 72. Note that the description is not a legal definition; rather, it serves to establish a conceptual scenario for consideration in identifying applicable countermeasures. The security organization should cross-reference each undesirable event with the security criteria that mitigate it. Undesirable events that are marked with a "Y" (yes) and colored red are generally mitigated by the corresponding countermeasure; those with an "N" (no) are not.

For events not identified in the tables in Section 7.0, the ISC recommends that agencies add customized undesirable events and either relate them to countermeasures in the tables or develop a specialized set of countermeasures for the additional events.

The list of undesirable events is not necessarily all inclusive. Unique facilities may face other mission-specific threats. For events not identified in the tables in Section 7.0, the ISC recommends that agencies add customized undesirable events and either relate them to countermeasures in the tables or develop a specialized set of countermeasures for the additional events (in addition to those included in this Standard). For example, a biological research laboratory may establish tables to address contamination events, and identify corresponding containment measures.

For each undesirable event where the assessed risk is either less than or exceeds the baseline LOP, the security organization must identify the countermeasures that will provide an LOP equivalent to the level of risk. Level I—Minimum countermeasures are typically less stringent, but may also be less effective in mitigating higher risks; Level V—Very High countermeasures are typically more stringent, and generally more effective.

⇧ If the assessed risk is higher than the baseline LOP, select countermeasures from a higher LOP.

- Or -

⇩ If the assessed risk is lower than the baseline LOP, select countermeasures from a lower LOP.

A minimum level of risk should be mitigated by countermeasures from the Level I-Minimum column, a low level of risk should be mitigated by countermeasures from the Level II-Low column, and so on (Figure 11).

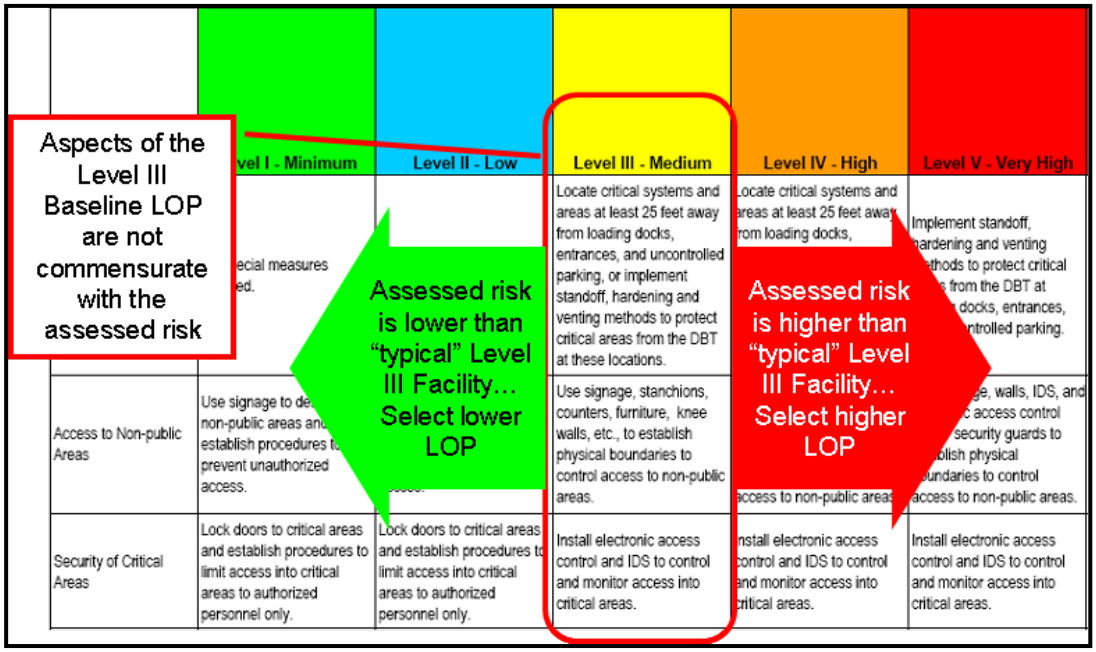


Figure 11. Adjusting From the Baseline LOP

By determining which countermeasures are applicable to the assessed risks and identifying changes from the baseline LOP, the necessary LOP can be developed. Continue to step 6.1.5.

6.1.5 Decision Point: Is the Existing LOP Sufficient?

Once the LOP necessary to meet the risk is identified, an evaluation of current conditions must be made to identify the existing countermeasures. In the case of new construction or developing a lease specification in a new facility, there are no existing countermeasures to evaluate, and thus no existing LOP. Continue to step 6.1.6.

The existing LOP may be determined through site surveys, interviews, reviews of policies and procedures, "red team" testing, tabletop exercises, etc. to determine what countermeasures are currently in place and how effective they are. Current conditions may then be matched up against the countermeasure criteria tables in Section 7.0 The existing LOP is then compared to the necessary LOP to determine if it adequately addresses the threat(s), or if vulnerabilities need to be addressed.

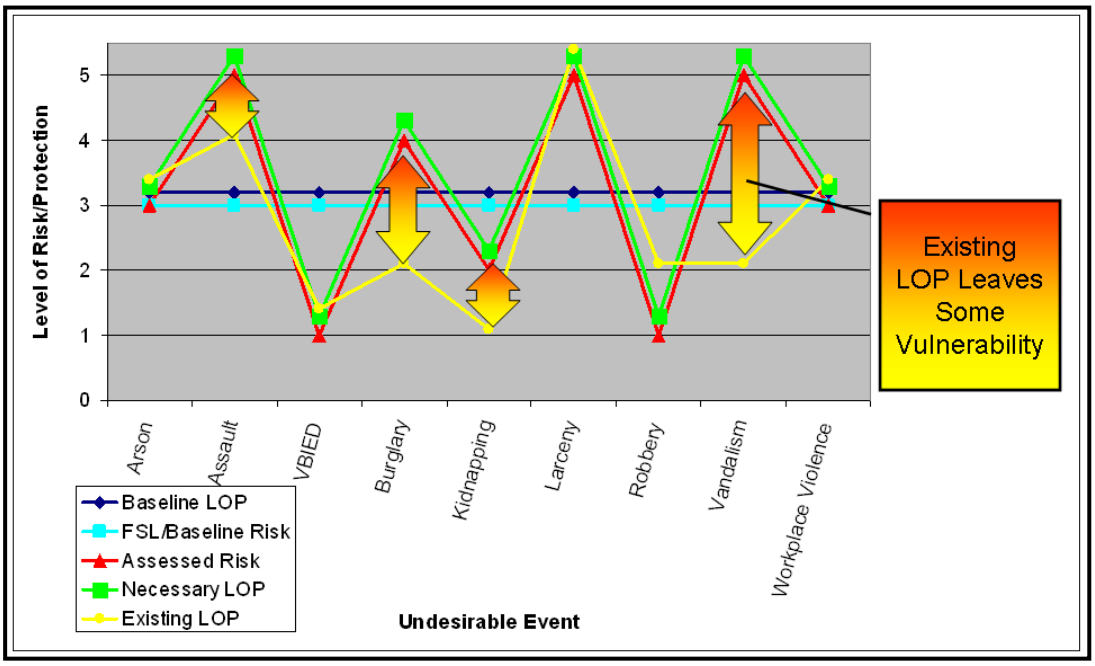


Figure 12. Existing LOP Compared to Necessary LOP

- If the existing LOP equates to the necessary LOP, current countermeasures should be maintained and tested on a regular basis. Conditions at the facility should be monitored for changes that may impact the effectiveness of countermeasures or the needed LOP.

- Or -

- If the existing LOP does not sufficiently address the risks, shortfalls must be identified and countermeasures to address those vulnerabilities must be considered for implementation. Continue to Step 6.1.6.

6.1.6 Decision Point: Is the LOP Achievable?

If the existing LOP is insufficient, a determination must be made as to whether the necessary LOP can be achieved; specifically, if the countermeasure can be physically implemented, and whether the investment is cost effective. Cost effectiveness is based on the investment in the countermeasure versus the value of the asset. In some cases, investment in an expensive countermeasure may not be advisable because the lifecycle of the asset is almost expired. Additionally, consideration should be given to whether other countermeasures may take priority for funding.

Note that "cost-effective" is a different determination than "cost-prohibitive." A countermeasure is cost-prohibitive if its cost exceeds available funding. Funding may exist for a countermeasure, but it may not be a sound financial decision to expend that money for little gain, making it not cost-effective.

New construction, with few exceptions, is fully expected to meet the LOP. In some cases, site limitations may restrict standoff distances, or fiscal limitations may prohibit the implementation of some measures; both examples illustrate why the security requirements should be identified as early in the process as possible (see Section 6.2.1). During the design process, there is a point where design changes are cost-prohibitive and make the LOP unachievable.

During the lease process, it may be determined that available facilities in the delineated area cannot meet the requirements of the LOP. This may be determined through a market survey, or when responses to a solicitation do not meet the requirements specified to meet the LOP.

In an existing leased facility, the terms of the lease might not allow the implementation of certain countermeasures that impact the entire facility.

In an existing facility, physical limitations and budgetary restrictions may make the LOP unachievable. For example, additional standoff distance might not be available; upgrade of window systems to resist blast pressure might require

complete renovation of the façade so that the window system will stay attached to the walls and thus be cost-prohibitive; or the current design of the air handling system could prohibit relocation of air intakes to a less vulnerable area.

Cost considerations could also be a primary factor in a decision not to implement a recommended countermeasure, or a decision to defer a funding request until such time as the likelihood of obtaining funding is more favorable. This Standard does not mandate the use of a specific cost analysis methodology. However, all costs, including life-cycle costs, shall be considered in whatever cost analysis methodology is used. In addition to direct project costs, those costs associated with indirect impacts (e.g., business interruption, relocation costs, or road closures) should be considered. Any decision to reject implementation outright or defer implementation due to cost (or other factors) must be documented, including the acceptance of risk.

This Standard does not mandate the use of a specific cost analysis methodology. However, all costs, including life-cycle costs, shall be considered in whatever cost analysis methodology is used.

- If the appropriate LOP is achievable, a timetable for implementation must be considered. Go to step 6.1.11.

- Or -

- If the appropriate LOP is not achievable, the highest achievable LOP must be identified. Continue to step 6.1.7.

6.1.7 Determine the Highest Achievable LOP

If the FSC has determined that the necessary LOP cannot be implemented, the highest achievable LOP must be identified. This may require an iterative process of examining the countermeasures included in the next lower LOP, determining if they are achievable, and if not, repeating the process with the next lower LOP. This approach minimizes the amount of risk that might be accepted (Figure 13).

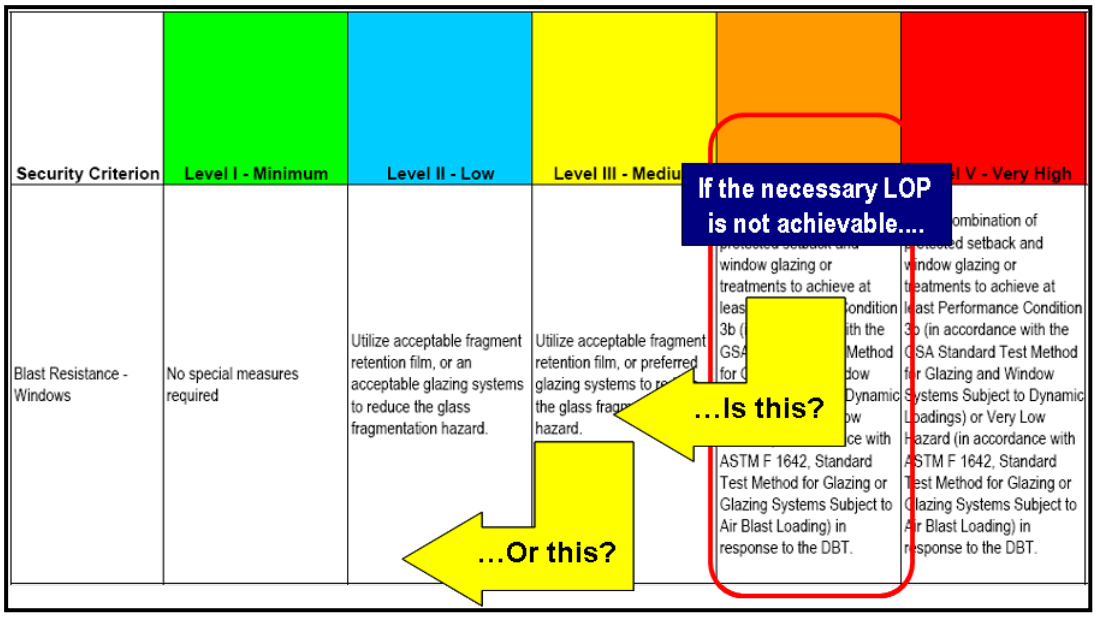


Figure 13. Minimizing Risk Acceptance by Implementing an Achievable LOP

For example, an assessment may determine that the risk of a hazardous substance being introduced into ground-level air intakes may be high and that the Level IV-High LOP calls for the air intakes to be relocated to the rooftop or a high wall. In an existing federal facility, the configuration of the air handling system in an existing facility may make a retrofit cost-prohibitive or even physically impossible. In a lease process, it might be determined during the market survey that no facilities in the delineated area have such a configuration. The Level III-Medium LOP calls for monitoring of the ground-level air intakes with closed-circuit television (CCTV) and guard patrols. If that is technologically and financially feasible, or available within the delineated market area, it would be further considered for implementation.

The project documentation must clearly reflect any reason why the necessary LOP cannot be achieved.

Continue to step 6.1.8.

6.1.8 Decision Point: Is the Risk Acceptable?

If the necessary LOP cannot be achieved, consideration must be given to the amount of risk that would be accepted given the highest achievable LOP. The difference between the protection afforded by the necessary LOP and the reduced protection afforded by the achievable LOP is the risk that must be accepted (Figure 14).

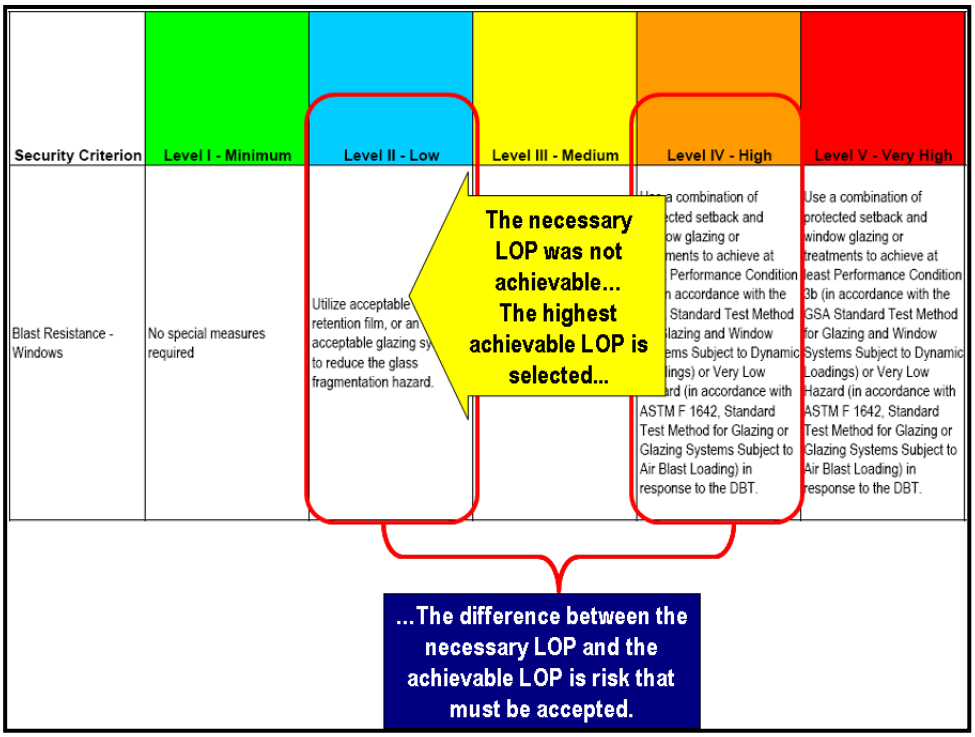


Figure 14. Risk Acceptance

It is impossible to establish a "rule of thumb" identifying how many LOPs below the necessary LOP is "acceptable." Specific conditions ─ site, budget, political, etc.─ will dictate the achievable LOP in each situation. The amount of risk to be accepted must be minimized through the iterative process described here. Regardless of site conditions, the LOP implemented may never be less than Level I-Minimum.

- If the amount of risk left unmitigated by the highest achievable LOP is acceptable, go to step 6.1.10.

- Or -

- If the amount of risk left unmitigated by the highest achievable LOP is not acceptable, continue to step 6.1.9.

6.1.9 Decision Point: Are Alternate Locations Available?

If the necessary LOP cannot be achieved and the risk that remains given the highest achievable LOP is not acceptable, consideration must be given to identifying an alternate location where the necessary LOP can be achieved (including the possibility of a new lease construction, or of expanding the delineated area). Inherent in this process is an assessment in the potential facility to ensure it can meet the LOP. Factors to be considered when determining if an alternate location is an option include:

- Limitations on the delineated area;
- Mission needs;
- Market conditions;
- Time frame;
- Budget; and,
- Other operational requirements.

If alternate locations are available, they must be evaluated to determine if any different risks are inherent in that location, and if the necessary LOP can be achieved. While the original security requirements would generally still be applicable, site specific conditions must be evaluated to determine if there is a change in the nature of risks at the alternate facility. For example, an alternate facility might be in a higher crime area, necessitating additional measures to prevent burglary.

In many situations an alternate location is not feasible. For example, if the tenant is already in an existing building, budgetary constraints may prohibit relocation. Similarly, available sites for new construction may have limitations (again, security should be a part of the design requirements phase so that it is considered in site selection). In many cases the mission of the tenant (such as the Census Bureau or Social Security offices) dictates that the facility be in a specific delineated area, which limits the availability of alternate sites.

- If alternative locations are available, they must be evaluated to determine if any different risks are inherent in that location, and if the necessary LOP can be achieved. Return to step 6.1.2 for each potential facility.

- Or -

- If the alternate location is not feasible, some risk will have to be accepted, and a lower LOP must be implemented. Continue to step 6.1.10.

6.1.10 Accept Risk

The acceptance of risk is an allowable outcome of applying this risk management process.

The acceptance of risk is an allowable outcome of applying this risk management process.

Though made every day in government, the decision to accept risk is not one to be taken lightly. The threat to Federal facilities is very real, and the decision to accept risk could have very real consequences. For that reason, it is critical that decision-makers obtain all the information they deem necessary to make a fully informed decision.

In some cases, accepting risk is unavoidable. Multiple competing requirements, standards, and priorities cannot always be reconciled. All budgets have some limitation; political and mission requirements cannot be ignored.

In all cases, the project documentation must clearly reflect the reason why the necessary LOP cannot be achieved. It is extremely important that the rationale for accepting risk be well-documented, including alternate strategies that are considered or implemented, and opportunities in the future to implement the necessary LOP. See Appendix D, Sample Risk Acceptance Justification Template, for an example of how the acceptance of risk might be documented. Follow ISC FSC guidance regarding retention and documentation of decision making.

The project documentation must clearly reflect the reason why the necessary LOP cannot be achieved.

Once a credible and documented risk assessment has been presented to and accepted by the decision maker(s), the security provider is not liable for any future decision to accept risk. This does not exempt the security provider from their liability associated with the accuracy and completeness of the risk assessment itself or from implementation of countermeasures.

At this point, a customized LOP for the facility has been developed: risks have been assessed, an achievable LOP has been identified, and risks that will be accepted have been documented. Now it is necessary to determine if the customized LOP is achievable immediately. Continue to step 6.1.11.

6.1.11 Decision Point: Is the LOP Achievable Immediately?

The amount of preparation required to implement a countermeasure may limit its immediate achievability. If a countermeasure is no-cost (such as a procedural change) or can be incorporated into an ongoing or planned project (such as a lobby redesign), or if funding is available, the countermeasure can generally be implemented immediately. When countermeasures require advance budgeting or coordination with owners and outside authorities for approval, implementation may be delayed.

In the case of new construction, countermeasures will be integrated into the design and implemented during construction. In leases, some countermeasures may require coordination with the lessor and perhaps other nongovernmental tenants. In existing buildings, delayed implementation is often necessary when the LOP requires funding that is not available within the current fiscal year budget resources, or coordination among multiple government tenants. See Section 6.2 for specific implementation under various circumstances.

- If the necessary LOP is immediately achievable, the countermeasures should be implemented. Go to step 6.1.13.

- Or -

- If the necessary LOP is not immediately achievable, the delayed implementation must be planned and interim countermeasures shall be implemented to temporarily mitigate the risks. Continue to step 6.1.12.

Interim countermeasures shall be considered when risk has been identified but the permanent countermeasures to mitigate it are not achievable immediately.

6.1.12 Implement Interim Countermeasures

Interim countermeasures shall be considered when risk has been identified but the permanent countermeasures to mitigate it are not immediately achievable. Interim countermeasures may involve establishing temporary procedures, posting additional guards, or utilizing portable equipment. The countermeasures may provide a similar or even equivalent LOP. For example, “Jersey barriers” or “K-rails” may meet vehicle barrier requirements but ultimately be replaced by permanent barriers that match the facility design. In other cases, interim countermeasures may provide less protection but still mitigate the risk to a reasonable degree until the full LOP can be achieved. For example, a visual

inspection of identification badges may be implemented until an electronic access control system can be installed.

The countermeasures identified through the application of this Standard as necessary and achievable must ultimately (and as rapidly as possible) replace any interim countermeasures. A plan for future permanent replacement must accompany any implementation of interim countermeasures. Go to step 6.1.13.

6.1.13 Implement Permanent Countermeasures

Once the customized LOP is established, it must be implemented. Appendix A, Details of Security Measures, provides specific information regarding implementation.

6.2 Application to Project-Specific Circumstances

The following describes how the process defined in Section 6.1 is applied to various project-specific circumstances.

6.2.1 Application to New Construction

As with previous ISC standards, the implementation of this Standard does not preclude new construction in urban environments, although it may require the acceptance of some risk. In these cases, the acceptability of risk is balanced against the needs of the tenant and how dependent the mission is on the location of a facility.

For buildings to be constructed (whether lease-construct or Government-owned), this Standard shall be applied as part of the requirements-definition process.

For buildings to be constructed (whether lease-construct or Government-owned), this Standard shall be applied as part of the requirements-definition process. The security organization will conduct a project-specific risk assessment during the requirements definition phase and recommend countermeasures and design features to be included in the design specifications. The FSC will determine whether the identified countermeasures will be implemented or risk will be accepted. Those countermeasures will become part of the facility's design program requirements to ensure that required security measures are fully integrated into the configuration of the site and/or building design.

Site security requirements for new construction, particularly setback, must be identified before a site is acquired and the construction funding request is finalized. This may prevent the selection of a site that lacks necessary features, especially sufficient setback, and help reduce the need for more costly countermeasures such as blast hardening.

6.2.2 Application to Existing Federal Facilities

For existing buildings this Standard shall be applied as part of the periodic risk assessment process.

For existing Federal facilities (leased or Government-owned), this Standard shall be applied as part of the periodic risk assessment process. The security organization will conduct a periodic risk assessment (at the frequency specified by the ISC "Facility Security Level Determinations for Federal Facilities") and recommend countermeasures and design features to be implemented at the facility. The FSC will determine whether the recommended countermeasures will be implemented or if risk will be accepted.

For approved countermeasures that cannot be implemented immediately, a plan to phase in countermeasures and achieve compliance shall be instituted. In some cases, the implementation of countermeasures must be delayed until renovations or modernization programs occur.

Historic buildings are addressed in the same manner as other existing buildings. Compliance with Section 106 of the National Historic Preservation Act is governed by U.S. Department of Interior regulations found in 36 CFR Part 800 and must be coordinated with the State Historic Preservation Officer consistent with established agency/departmental implementing procedures. Design alternatives for incorporating the necessary security measures into the historic property should be fully explored with a design professional to balance historic preservation goals and security requirements.

6.2.3 Modernization and Renovation

For buildings identified to undergo a renovation or major modernization, this Standard shall be applied during the planning and prospectus development phase.

When a renovation or major modernization of an existing facility is initiated, many of the countermeasures which were previously deemed "not achievable" due to facility limitations or funding considerations may now be achievable as part of the project. For buildings identified to undergo a renovation or major modernization, this Standard shall be applied during the planning and prospectus development phase.

Specifically, the following applies:

- When an existing building is being renovated, the security organization will conduct a project-specific risk assessment during the requirements definition phase. Prior security assessments and delayed implementation plans shall be reviewed to identify countermeasures that were deferred because of facility constraints or cost considerations.

- When an existing building or space is to have a change in building occupancy type (e.g., a warehouse is converted to office space), the security organization will conduct a project-specific risk assessment representative of the finished

building or space during the requirements definition or concept phase.

- Additions to existing buildings shall be designed and constructed to comply with this Standard. The security organization will conduct a project-specific risk assessment for the addition. If the addition is 50 percent or more of the gross area of the existing building, this Standard shall be applied to the entire building (existing portions and the addition).

In all cases, the FSC will still determine whether the recommended countermeasures will be implemented as part of the modernization or the risk will continue to be accepted. Approved countermeasures will be incorporated into the project program and prospectus proposal.

6.2.4 Application to Lease Solicitations

As with previous ISC standards, the implementation of this Standard does not preclude leasing in urban areas.

Unless there is a change in tenant(s) or mission, this Standard does not apply to renewals, extensions, expansions, superseding leases, and succeeding leases that are established through other than full and open competition, but is recommended. If there is a change in tenant(s) or mission, this Standard does apply (see Sections 6.2.5 and 6.2.6).

For renewals, extensions, expansions, superseding leases, and succeeding leases that are established through other than full and open competition, the requirement to change the security countermeasures will not apply during the procurement process.

Otherwise, for these types of leasing actions the FSL determinations and risk assessments will continue to be done in accordance with the schedule established for the facility.

For new lease acquisitions, lease-construction, and succeeding leases that are established through full and open competition, this Standard shall be applied during the requirements definition, negotiation and build-out phases. The security organization will conduct a project-specific FSL assessment and risk assessment during the requirements definition phase and recommended counter measures and security design features will be included in the lease solicitation. Security requirements must be applied equally to all offers in the procurement.

Market surveys will provide the prospective tenant and the leasing agency (if different from the tenant agency) with information regarding whether the LOP can be achieved in the delineated area. Any additional risks identified and any additional countermeasures or design features identified by the security organization will be presented to the FSC for a determination of whether to implement in the requirements of the solicitation or accept the risk. If the required LOP cannot be met in the delineated area, the

prospective tenant(s) and leasing agency will determine whether to change the delineated area or have the FSC reassess the minimum security requirements. As described in section 6.1.9, other factors affecting the feasibility of altering the delineated area, such as mission needs, market conditions, time frame, budget and operational considerations, may be taken into account.

For new lease acquisitions, lease construction, and succeeding leases that are established through full and open competition, this Standard shall be applied during the requirements definition, negotiation and build-out phases.

The security organization will evaluate the offerors' proposed security plans for effectiveness in meeting the LOP required.

The security organization will update the risk assessment on offers in the competitive range to identify threats and vulnerabilities for the specific properties and recommend any additional security measures. The FSC will determine which of the additional recommended security measures will be adopted and/or accept the risk. The leasing agency (if different from the tenant agency) will determine how the additional countermeasures will be implemented in the procurement. Major items may have to be included as an amendment to the solicitation. Minor items and quantitative changes may be able to be presented to the individual offerors prior to final proposal revisions, or included in the build-out phase post award.

Should none of the offers received meet the minimum security requirements of the solicitation, the prospective tenant(s) and leasing agency shall consider expanding the delineated area or have the FSC reassess the minimum security requirements. As described in section 6.1.9, the feasibility of altering the delineated area may be taken into account.

During the build-out phase of the lease, the security organization will conduct an inspection of the leased space for proper installation and functionality of the security systems and countermeasures.

6.2.5 Tenant and Mission Changes in Occupied Buildings

If a new tenant or change in the mission of an existing tenant brings new or increased risks, recommended countermeasure upgrades must be considered prior to the change.

Whenever consideration is given to moving new tenants (including outleases or backfilling vacant space) into a building that is already occupied by a Government tenant, the potential for increasing security requirements — and impacts on the funding and operations of the existing tenants— must be a part of the decision process. Moving a higher-risk tenant into a facility already occupied by a government tenant with lower security requirements brings with it inherent challenges in sharing funding, making decisions on accepting risk and responsibility for implementation.

Changes to the mission of an existing tenant brings with it even greater challenges in making decisions on accepting risk and responsibility for implementation than moving in a new tenant. The decision to change the mission of an existing tenant ─ and possibly increase the risks to the facility and the cost for increased security─ is typically made solely by the tenant Department or Agency, without input from or consideration for the other tenants.

Conversely, changing a tenant's mission to a lower-risk mission, or moving a high-risk tenant out of a facility could reduce the risk to the remaining tenants. Some countermeasures could be decomissioned or reduced.

In these cases, the security organization must assess the entire facility with respect to changes to the risk to the facility that would be created by the presence of a new tenant or the changing mission of an existing one. The security organization should assess the overall FSL for the facility and make a new determination as necessary. If the FSL remains the same, the adequacy of the existing countermeasures should be reviewed and appropriate security enhancements implemented. If the FSL changes, a new risk assessment and analysis of the baseline LOP is required, including customization analysis, as outlined in Section 6.1. If new or increased risks are identified, recommended countermeasure upgrades must be considered prior to the change. Any recommended changes to security must be considered by the FSC, prospective new tenant or tenant with the mission change, and the leasing or owning agency.

A plan to phase in countermeasures and achieve compliance may be necessary, particularly where cost-sharing agreements must be developed.

6.2.6 Campus Environments

In a campus environment, site-specific conditions will dictate how campus-wide countermeasures impact individual facilities and exterior restricted areas. The FSC should consider the campus security characteristics when the baseline security countermeasures are established for each facility within the campus.

For example, the characteristics of a facility located within the confines of a campus may require visitor vehicles be screened prior to entering the parking garage. If visitor vehicles are screened prior to entering the campus, additional screening prior to entering the parking garage of a specific building is not necessary.

Conversely, restricted areas within the campus, such as employee-only parking, utility buildings, and other buildings or improvements within the campus itself, may still require enclosures or other protective measures.

In applying the security criteria contained in this Standard, the security organization should exercise sound judgment in identifying security measures necessary at individual buildings. It may be more cost-effective to implement security measures at the perimeter, precluding the necessity to duplicate security measures at individual buildings or areas within the campus.

6.2.7 Purchases

For buildings to be purchased, this Standard shall be applied as part of the requirements-definition process. The security organization will conduct a project-specific risk assessment during the requirements definition phase. Recommended countermeasures and design features must be considered as part of the project cost and included in the scope of work needed to make the building suitable for occupancy.

The tenant representatives to the project team will determine whether the recommended countermeasures will be implemented or the risk will be accepted.

In the case of buildings contemplated for purchase, the security measures should be considered as part of the project cost and included in the scope of work needed for making the building suitable for occupancy.

7.0 Security Criteria

The following tables identify the security measures to be applied as part of the baseline LOP or a customized LOP:

- Site—including the site perimeter, site access, exterior areas and assets, and parking.
- Structure—including structural hardening, façade, windows, and building systems
- Facility Entrances—including employee and visitor pedestrian entrances and exits, loading docks, and other openings in the building envelope;
- Interior—including space planning and security of specific interior spaces;
- Security Systems—including intrusion-detection, access control, and closed circuit television camera systems; and,
- Security Operations and Administration—including planning, guard-force operations, management and decision-making, and mail handling and receiving.

7.1 Format of the Tables

The tables are organized to provide a user-friendly cross-reference from the countermeasures and baseline LOPs to the undesirable events used for customization. Each table identifies security criteria in the first (left) column followed by their degree of applicability or specificity of countermeasures at each of the five security levels in the next five columns. The facing page of each table identifies the corresponding undesirable events that each countermeasure commonly addresses, for reference when customizing the LOP (Figure 15).

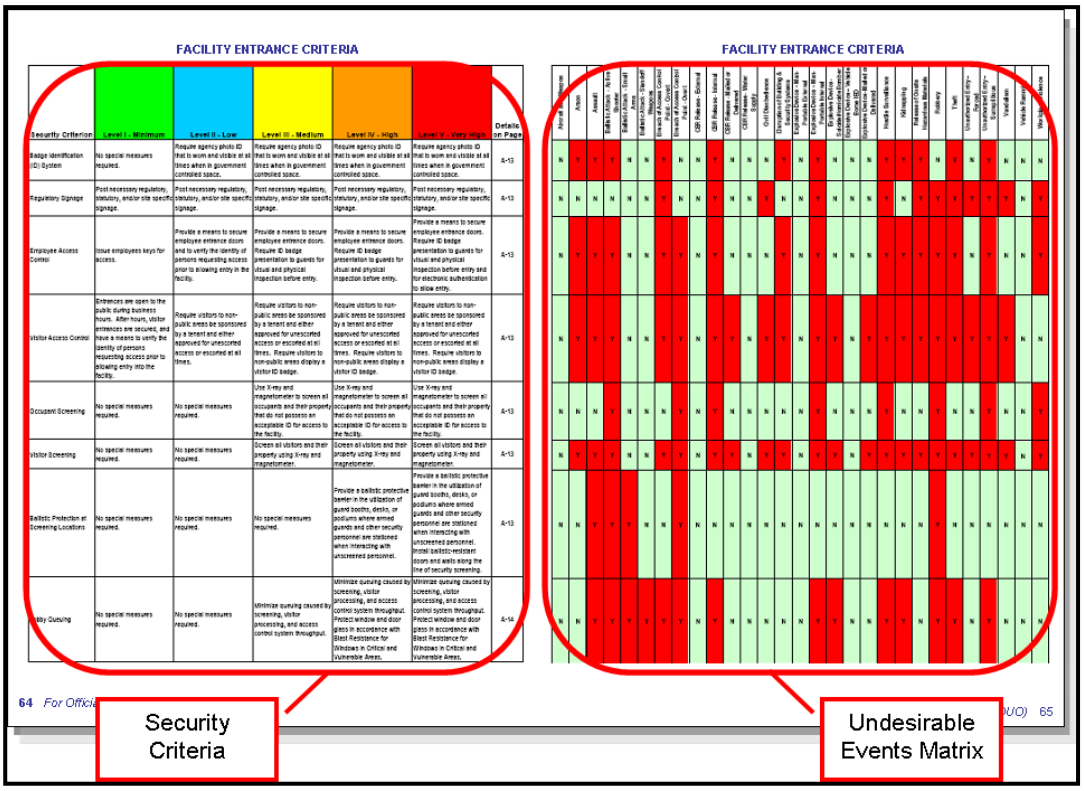


Figure 15. Countermeasure Table Layout

In many instances, the degree of applicability increases from a lower FSL to a higher FSL. The countermeasures are generally cumulative as the LOP increases (i.e., to achieve the Medium LOP, the countermeasures in Minimum, Low, and Medium must be implemented). However, when in conflict, the higher LOP supersedes the lower (e.g., if the Medium LOP requires a fence and the High LOP requires a wall, only the wall would be implemented).

In some cases, the security criteria may be "not applicable," for example when no underground parking exists, or there are no restricted areas on the outside of the building. In this case, documentation should reflect the criteria as "not applicable," not as "met" or "compliant."

Appendix A provides details on implementation and other considerations for each security criterion. While the application of security measures at the various levels is specific, this Standard does not recommend specific technologies, systems, or manufacturer brands. Selection of individual systems and technologies is at the discretion of the Department and Agency security organizations.

The tables do not contain specific technologies, systems, or manufacturer brands. Selection of individual systems and technologies are to be determined by the Department and Agency security organizations.

7.2 Design-Basis Threat

A design-basis threat (DBT) is a profile of the type, composition, and capabilities of an adversary used for security planning. In some instances, specific information about the threat may be required to determine which LOP to implement (e.g., when to deploy CCTV cameras) or to develop a performance specification (e.g., the size of an explosive device to protect against). To support such determinations, and to maintain additional control of sensitive threat assessment information, the ISC has developed a companion document to this Standard, "The Design-Basis Threat."

Security organizations and decision-making officials should reference the most current edition of "The Design Basis Threat," unless an agency-specific threat assessment publication is available.

"The Design-Basis Threat" is an ISC report developed in cooperation with various Government intelligence organizations. The document provides a basis for decision-making, including the assignment of threat ratings and the relative prioritization of threats. The ISC will update the document on a regular basis to ensure that it contains the most current information.

In implementing this Standard, security organizations and decision-making officials should reference the most current edition of "The Design-Basis Threat," unless an agency-specific threat assessment publication is available.

In order to keep pace with the changing nature of the threat to Federal facilities, updates to "The Design-Basis Threat" will be made periodically. Users should visit the ISC Web site (www.dhs.gov/isc) for the latest edition.

7.3 Establishing LOP Templates

Some Departments and Agencies construct or acquire similar facilities to accomplish identical missions in various locations. For example, GSA constructs child-care centers (CCCs) across the nation. CCCs generally face similar threats that can be mitigated by a similar LOP at each location. Instead of repeating the entire customization process for each child care center, an LOP template can be developed and applied to all CCCs.

The LOP template would serve as a boilerplate set of security requirements to be incorporated into the development of these facilities. In essence, the agency is creating a security design guide, starting with the selection of a common LOP. The LOP template avoids replication of the customization process, shortens the lead time required to identify security requirements when new projects are initiated, serves as the basis for cost-estimating, and encourages standardization across common facility types.

To create a LOP template, a common risk assessment must be developed that applies to all facilities in a common category. A customized LOP is then developed following the processes discussed in Section 6.1. The countermeasure selections in the customized LOP then become the LOP template (Figure 16). In all cases, a site-specific assessment should be conducted to ensure that any additional risks not covered by the LOP template are appropriately mitigated by measures beyond those specified in the template.

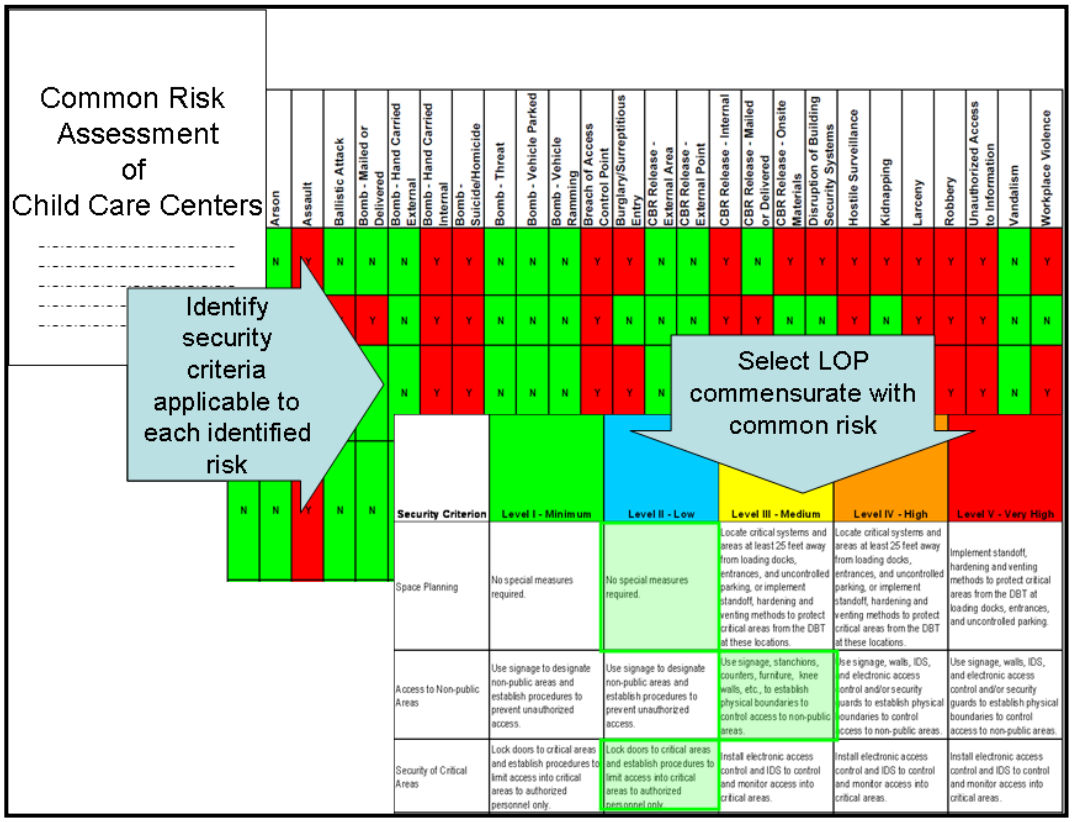


Figure 16. Developing an LOP Template

Where appropriate, the ISC may adopt these LOP templates as annexes to the ISC's compendium of standards, indicating concurrence that the templates are compliant with ISC standards.

Annex 1 to this Standard, "Child-Care Center LOP Template," includes the boilerplate requirements for child-care centers in Federal facilities and may be used as an example for further templates.

This Page Intentionally Left Blank

Security Criteria Tables

Index of Criteria

SITE SECURITY CRITERIA

Security Criterion	Level I - Minimum	Level II - Low	Level III - Medium	Level IV - High	Level V - Very High	Details on Page
Identification as Federal Facility	No special measures required.	Signage identifying a facility as a Federal facility should only be posted when necessary to achieve the mission of the tenants, or when the facility is readily identified or well-known as a government facility based on the nature of public contact or other operations.	Signage identifying a facility as a Federal facility should only be posted when necessary to achieve the mission of the tenants , or when the facility is readily identified or well-known as a government facility based on the nature of public contact or other operations.	Signage identifying a facility as a Federal facility should only be posted when necessary to achieve the mission of the tenants , or when the facility is readily identified or well-known as a government facility based on the nature of public contact or other operations.	Signage identifying a facility as a Federal facility should only be posted when necessary to achieve the mission of the tenants , or when the facility is readily identified or well-known as a government facility based on the nature of public contact or other operations.	A-3
Landscaping	Minimize areas of concealment in and around facilities.	Restrict landscaping from obstructing views of the security guards and CCTV cameras, or interfering with lighting or IDS.	Restrict landscaping from obstructing views of the security guards and CCTV cameras, or interfering with lighting or IDS.	Restrict landscaping from obstructing views of the security guards and CCTV cameras, or interfering with lighting or IDS.	Restrict landscaping from obstructing views of the security guards and CCTV cameras, or interfering with lighting or IDS.	A-3
Pedestrian Access to Site	No special measures required.	No special measures required.	No special measures required.	In a campus environment, install fence, landscaping, or other barriers to channel pedestrians to authorized areas or entrances.	Install fence, landscaping, or other barriers to channel pedestrians to authorized areas or entrances.	A-3
Vehicle Access Points	No special measures required.	No special measures required.	Limit the number of vehicle access points.	Limit the number of vehicle access points.	Limit the number of vehicle access points.	A-3
Site Lighting	Install exterior lighting at entrances and exits.	Install exterior lighting at entrances, exits, parking lots, and garages.	Install exterior lighting at entrances, exits, parking lots, garages, and walkways from parking areas to entrances.	Install exterior lighting at entrances, exits, parking lots, garages, and walkways from parking areas to entrances.	Install exterior lighting at entrances, exits, parking lots, garages, walkways from parking areas to entrances, and around building perimeter areas.	A-4
Restricted Areas	No special measures required.	Use trees, hedges, berms, or any combination of these elements to create buffer zones to separate public areas and other functions.	Provide fences, walls, gates or other barriers to prevent unauthorized access to restricted areas.	Provide fences, walls, gates or other barriers to prevent unauthorized access to restricted areas, and monitor with CCTV or guard patrols.	Provide fences, walls, gates or other barriers to prevent unauthorized access and observation to restricted areas, and monitor with CCTV or guard patrols.	A-4
Signage - Sensitive Areas	No special measures required.	Prohibit signs that identify sensitive areas, unless required by other standards/codes.	Prohibit signs that identify sensitive areas, unless required by other standards/codes.	Prohibit signs that identify sensitive areas, unless required by other standards/codes.	Prohibit signs that identify sensitive areas, unless required by other standards/codes.	A-4
Control of Parking	No special measures required.	No special measures required.	Control vehicle access to underground/in-building parking.	Control vehicle access to underground/in-building parking and on-site surface or structured parking.	Control vehicle access to the area required to meet the setback from the DBT.	A-4
Authorized Parking	No special measures required.	No special measures required.	Limit parking to employee vehicles, authorized visitor vehicles, approved government vehicles, and other authorized parkers.	Limit parking to employee vehicles, screened visitor vehicles, and approved government vehicles.	Limit parking to employee vehicles, screened visitor vehicles, and approved government vehicles.	A-4

SITE SECURITY CRITERIA

Aircraft as a Weapon	Arson	Assault	Ballistic Attack - Active Shooter	Ballistic Attack - Small Arms	Ballistic Attack - Standoff Weapons	Breach of Access Control Point - Covert	Breach of Access Control Point - Overt	CBR Release - External	CBR Release - Internal	CBR Release - Mailed or Delivered	CBR Release - Water Supply	Civil Disobedience	Disruption of Building & Security Systems	Explosive Device – Man-Portable External	Explosive Device – Man-Portable Internal	Explosive Device - Suicide/Homicide Bomber	Explosive Device – Vehicle Borne IED	Explosive Device - Mailed or Delivered	Hostile Surveillance	Kidnapping	Release of On-site Hazardous Materials	Robbery	Theft	Unauthorized Entry – Forced	Unauthorized Entry – Surreptitious	Vandalism	Vehicle Ramming	Workplace Violence
Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
N	Y	Y	N	Y	N	N	N	Y	N	N	Y	N	Y	Y	N	N	N	N	Y	Y	Y	Y	N	Y	Y	Y	N	N
N	Y	Y	Y	Y	Y	N	N	Y	N	N	Y	Y	N	Y	N	Y	N	N	Y	Y	Y	Y	Y	Y	Y	Y	N	N
N	N	Y	Y	Y	Y	N	N	Y	N	N	N	Y	N	Y	N	N	Y	N	Y	Y	Y	N	N	Y	Y	Y	Y	N
N	Y	Y	N	Y	N	N	N	Y	N	N	Y	N	Y	Y	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	N	N
N	Y	N	N	N	N	N	N	Y	N	N	Y	N	Y	Y	N	N	Y	N	Y	N	Y	N	N	Y	Y	N	N	N
N	Y	N	N	N	N	N	N	Y	N	N	Y	N	Y	Y	N	N	Y	N	Y	N	Y	N	N	Y	Y	N	Y	N
N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	Y	Y	N	N	Y	N	N
N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N

SITE SECURITY CRITERIA

Security Criterion	Level I - Minimum	Level II - Low	Level III - Medium	Level IV - High	Level V - Very High	Details on Page
Vehicle Access to Controlled Parking	No special measures required.	Designate employee and visitor parking areas.	Use vehicle gates to limit access of vehicles to authorized vehicles only.	Provide vehicle barriers to protect parking entrances from penetration by a vehicle meeting the DBT.	Provide vehicle barriers to protect parking entrances from penetration by a vehicle meeting the DBT. Vehicle entrances shall be staffed by a guard who has the ability to raise the barriers quickly in an emergency, or utilize a dual-barrier vehicle trap system to prevent piggybacking.	A-5
Vehicle Barriers	No special measures required.	No special measures required.	Provide vehicle barriers to protect pedestrian entrances from penetration by a vehicle meeting the DBT.	Provide vehicle barriers to protect pedestrian and vehicle access points, and critical areas/utilities from penetration by a vehicle meeting the DBT.	Provide vehicle barriers around the entire facility at the established setback distance from penetration by a vehicle meeting the DBT.	A-5
Vehicle Screening	No special measures required.	No special measures required.	Screen visitor vehicles before entry into the controlled parking area.	Screen visitor vehicles before entry into the controlled parking area. Randomly screen employee and contractor vehicles during heightened security alerts.	Screen visitor vehicles before entry into the controlled parking area. Randomly screen employee and contractor vehicles during heightened security alerts.	A-5
Pedestrian Access to Controlled Parking Areas	No special measures required.	Minimize areas of concealment in and around parking areas.	Monitor pedestrian access to parking areas.	Provide barriers to restrict pedestrian access into parking areas to authorized entry points.	Limit pedestrian access to controlled parking areas to authorized personnel only.	A-6
Hazardous Materials Storage	No special measures required.	Locate HAZMAT storage in a restricted area away from loading docks, entrances, and uncontrolled parking.	Locate HAZMAT storage in a restricted area away from loading docks, entrances, and uncontrolled parking.	Locate HAZMAT storage in a restricted area away from loading docks, entrances, and uncontrolled parking.	Locate HAZMAT storage in a restricted area away from loading docks, entrances, and uncontrolled parking.	A-6
Receptacle and Container Placement	No special measures required.	Position trash containers, mailboxes, vending machines, or other fixtures and features that could conceal devices away from building entrances.	Position trash containers, mailboxes, vending machines, etc. away from buildings, or implement blast containment measures to mitigate an explosion.	Position trash containers, mailboxes, vending machines, etc. away from buildings, or implement blast containment measures to mitigate an explosion.	Position trash containers, mailboxes, vending machines, etc. away from buildings, or implement blast containment measures to mitigate an explosion.	A-6

SITE SECURITY CRITERIA

Aircraft as a Weapon	Arson	Assault	Ballistic Attack - Active Shooter	Ballistic Attack - Small Arms	Ballistic Attack - Standoff Weapons	Breach of Access Control Point - Covert	Breach of Access Control Point - Overt	CBR Release - External	CBR Release - Internal	CBR Release - Mailed or Delivered	CBR Release - Water Supply	Civil Disobedience	Disruption of Building & Security Systems	Explosive Device – Man-Portable External	Explosive Device – Man-Portable Internal	Explosive Device - Suicide/Homicide Bomber	Explosive Device – Vehicle Borne IED	Explosive Device - Mailed or Delivered	Hostile Surveillance	Kidnapping	Release of On-site Hazardous Materials	Robbery	Theft	Unauthorized Entry – Forced	Unauthorized Entry – Surreptitious	Vandalism	Vehicle Ramming	Workplace Violence
N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N
N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N
N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N
N	Y	Y	N	N	N	N	N	Y	N	N	N	Y	N	Y	N	N	N	N	Y	Y	N	Y	Y	N	N	Y	N	N
N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	Y	N	N
N	Y	N	N	N	N	N	N	Y	N	N	N	N	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N

STRUCTURE SECURITY CRITERIA

Security Criterion	Level I - Minimum	Level II - Low	Level III - Medium	Level IV - High	Level V - Very High	Details on Page
Blast Resistance - Windows	No special measures required	Utilize acceptable fragment retention film, or an acceptable glazing systems to reduce the glass fragmentation hazard.	Utilize acceptable fragment retention film, or preferred glazing systems to reduce the glass fragmentation hazard.	Use a combination of protected setback and window glazing or treatments to achieve at least Performance Condition 3b (in accordance with the GSA Standard Test Method for Glazing and Window Systems Subject to Dynamic Loadings - see Appendix C) or Very Low Hazard (in accordance with ASTM F 1642, Standard Test Method for Glazing or Glazing Systems Subject to Air Blast Loading) in response to the DBT.	Use a combination of protected setback and window glazing or treatments to achieve at least Performance Condition 3b (in accordance with the GSA Standard Test Method for Glazing and Window Systems Subject to Dynamic Loadings - see appendix C) or Very Low Hazard (in accordance with ASTM F 1642, Standard Test Method for Glazing or Glazing Systems Subject to Air Blast Loading) in response to the DBT.	A-7
Blast Resistance - Façade and Structure	No special measures required	Use construction materials which have inherent ductility and which are better able to respond to load reversals (e.g., cast in place reinforced concrete column construction).	Use a combination of setback, site planning, façade hardening, and structural measures to provide a medium level of façade protection.	Use a combination of setback, site planning, façade hardening, and structural measures to provide a medium level of façade protection.	Use a combination of setback, site planning, façade hardening, and structural measures to provide a high level of façade protection.	A-8
Blast Resistance - Progressive Collapse	No special measures required	Use construction materials which have inherent ductility and which are better able to respond to load reversals (e.g., cast in place reinforced concrete and steel construction).	For buildings less than three stories, use a combination of setback, site planning, façade hardening, and structural measures to prevent progressive collapse from the DBT or the loss of any single exterior column or load-bearing wall, whichever is lower.	For buildings less than three stories, use a combination of setback, site planning, façade hardening, and structural measures to prevent progressive collapse from the DBT or the loss of any single exterior column or load-bearing wall, whichever is lower. Interior columns also shall be considered in buildings with an uncontrolled lobby.	For all buildings, regardless of number of stories, use a combination of setback, site planning, façade hardening, and structural measures to prevent progressive collapse from the DBT or the loss of any single column, whichever is higher.	A-9
Blast Resistance - Under-Building Parking	No special measures required.	Use construction materials which have inherent ductility and which are better able to respond to load reversals (e.g., cast in place reinforced concrete column construction).	Implement architectural or structural features, or other positive countermeasures (e.g., vehicle screening), that deny contact with exposed primary vertical load members in these areas. A minimum standoff of at least 150 mm (6 inches) from these members is required.	Utilize hardening and venting methods to limit airblast injuries in occupied areas from the DBT in a parking area. Significant structural damage to the walls, ceilings, and floors of the parking area may occur. However, the occupied areas above should not experience severe damage or collapse.	Design all columns in the garage area for an unbraced length equal to two floors, or three floors where there are two levels of parking.	A-9
Burglary Resistance of Windows	Lock all operable ground floor windows.	Lock all operable ground floor windows.	No operable windows on ground floor level.	No operable windows within 16 feet of the ground or other access point.	Design exterior windows in publicly accessible locations to resist forced entry.	A-9

STRUCTURE SECURITY CRITERIA

Aircraft as a Weapon	Arson	Assault	Ballistic Attack - Active Shooter	Ballistic Attack - Small Arms	Ballistic Attack - Standoff Weapons	Breach of Access Control Point - Covert	Breach of Access Control Point - Overt	CBR Release - External	CBR Release - Internal	CBR Release - Mailed or Delivered	CBR Release - Water Supply	Civil Disobedience	Disruption of Building & Security Systems	Explosive Device – Man-Portable External	Explosive Device – Man-Portable Internal	Explosive Device - Suicide/Homicide Bomber	Explosive Device – Vehicle Borne IED	Explosive Device - Mailed or Delivered	Hostile Surveillance	Kidnapping	Release of On-site Hazardous Materials	Robbery	Theft	Unauthorized Entry – Forced	Unauthorized Entry – Surreptitious	Vandalism	Vehicle Ramming	Workplace Violence
Y	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	N	Y	Y	N	N	N	N	N	N	N	N	N	N	N
Y	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	N	Y	Y	N	N	N	N	N	N	N	N	N	N	N
Y	N	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N
N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	Y	N	N	N	N	N	N	N	N	N	N	N
N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	Y	N	N	Y	Y	Y	Y	N	N

STRUCTURE SECURITY CRITERIA

Security Criterion	Level I - Minimum	Level II - Low	Level III - Medium	Level IV - High	Level V - Very High	Details on Page
Walls and nonwindow Openings	No special measures required.	No special measures required.	Protect nonwindow openings such as mechanical vents and exposed plenums to resist forcible entry.	Protect nonwindow openings such as mechanical vents and exposed plenums to resist forcible entry.	Protect walls and nonwindow openings in publicly accessible areas such as mechanical vents and exposed plenums to resist forcible entry.	A-10
Windows in Critical Areas - Ballistic Protection	No special measures required.	No special measures required.	Provide blinds, curtains, or other window treatments in critical areas that can be used to prevent visual observation into critical areas when temporary conditions warrant.	Prevent visual observation from the exterior into critical exterior offices.	Provide ballistic windows for critical exterior offices.	A-10
Protection of Air Intakes	Provide emergency shutdown, SIP, and evacuation procedures.	Provide emergency shutdown, SIP, and evacuation procedures, and secure accessible air intake grilles from tampering or removal.	Provide emergency shutdown, SIP, and evacuation procedures and protect accessible air intakes with fencing. Monitor with CCTV or guard patrols.	Provide emergency shutdown, SIP, and evacuation procedures, and place air intakes on rooftop or on wall at least 30 feet or three stories above grade.	Provide emergency shutdown, SIP, and evacuation procedures, and place air intakes on rooftop or on wall at least 30 feet or three stories above grade.	A-10
Isolated Ventilation Systems	No special measures required.	No special measures required.	Provide separate isolated HVAC systems in lobbies, loading docks, mailrooms and other locations susceptible to CBR attack that are isolated from other building areas.	Provide separate isolated HVAC systems in lobbies, loading docks, mailrooms and other locations susceptible to CBR attack that are isolated from other building areas. Ensure that the envelope of the isolated loading docks and mailrooms are full-height construction and are sealed to the floor, roof, or ceiling above.	Provide separate isolated HVAC systems in lobbies, loading docks, mailrooms and other locations susceptible to CBR attack that are isolated from other building areas. Ensure that the envelope of the isolated loading docks and mailrooms are full-height construction and are sealed to the floor, roof, or ceiling above. Provide instrumentation to monitor pressure relationship established by the isolated systems.	A-10
HVAC Control	No special measures required.	Develop written procedures for the emergency shut-down or exhaust of air handling systems.	Install an emergency shut-off and exhaust system for air handlers. Control movement of elevators, and close applicable doors and dampers to seal building.	Install a one-step shut-off and exhaust system for air handlers. Control movement of elevators, and close applicable doors and dampers to seal building. Provide an emergency response module to the buildings energy-management system to switch the system to a prescribed emergency response mode.	Provide two or more redundant locations for one-step shut-off or exhaust system for air handlers. Control movement of elevators, close applicable doors, and dampers to seal the building. Provide an emergency-response module to the buildings energy-management system to switch the system to a prescribed emergency-response mode.	A-10
CBR Detection Technology	No special measures required.	No special measures required.	No special measures required.	No special measures required.	Install CBR detection technology to protect critical areas against a known credible threat.	A-11

STRUCTURE SECURITY CRITERIA

Aircraft as a Weapon	Arson	Assault	Ballistic Attack - Active Shooter	Ballistic Attack - Small Arms	Ballistic Attack - Standoff Weapons	Breach of Access Control Point - Covert	Breach of Access Control Point - Overt	CBR Release - External	CBR Release - Internal	CBR Release - Mailed or Delivered	CBR Release - Water Supply	Civil Disobedience	Disruption of Building & Security Systems	Explosive Device – Man-Portable External	Explosive Device – Man-Portable Internal	Explosive Device - Suicide/Homicide Bomber	Explosive Device – Vehicle Borne IED	Explosive Device - Mailed or Delivered	Hostile Surveillance	Kidnapping	Release of On-site Hazardous Materials	Robbery	Theft	Unauthorized Entry – Forced	Unauthorized Entry – Surreptitious	Vandalism	Vehicle Ramming	Workplace Violence
N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	N	N
N	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N
N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N
N	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
N	Y	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
N	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N

STRUCTURE SECURITY CRITERIA

Security Criterion	Level I - Minimum	Level II - Low	Level III - Medium	Level IV - High	Level V - Very High	Details on Page
Biological Filtration - General Building	No special measures required.	No special measures required.	Use a Minimum Efficiency Reporting Value (MERV) 10 particulate filter on all exterior air handling units (AHUs).	Use a Minimum Efficiency Reporting Value (MERV) 13 particulate filter on all air handling units (AHUs), including the supply air stream for recirculating AHUs.	Use a HEPA filter or functional equivalent on AHUs serving critical areas.	A-11
Biological Filtration - Lobbies and Mailrooms	No special measures required.	No special measures required.	Use a Minimum Efficiency Reporting Value (MERV) 13 particulate filter on all air handling units (AHUs) in mailrooms and lobbies.	Use a Minimum Efficiency Reporting Value (MERV) 13 particulate filter on all air handling units (AHUs), including the supply air stream for recirculating AHUs in mailrooms and lobbies.	Use a HEPA filter or functional equivalent on AHUs serving mailrooms and lobbies, including outside ones, and in the supply air stream of recirculating AHUs.	A-11
Chemical Filtration	No special measures required.	No special measures required.	No special measures required.	No special measures required.	Provide gas adsorption filters on recirculated air as well as on outside air intakes which serve critical areas.	A-11
Security of Ventilation Equipment and Controls	No special measures required.	Protect the system controls from unauthorized access.	Protect the system controls from unauthorized access.	Provide IDS coverage of ventilation equipment and control rooms.	Provide IDS coverage and access control into ventilation equipment and control rooms.	A-11
Location of Utilities and Feeders	No special measures required.	No special measures required.	No special measures required.	Locate utility systems at least 25 feet away from loading docks, entrances, and uncontrolled parking, or implement standoff, hardening and venting methods to protect utilities from the DBT at these locations.	Locate utility systems at least 50 feet away from loading docks, entrances, and uncontrolled parking, or implement standoff, hardening and venting methods to protect utilities from the DBT at these locations.	A-11
Separation of Emergency and Normal Power Distribution	No special measures required.	No special measures required.	No special measures required.	Install emergency and normal power distribution systems (including electric panels, conduits, and switchgears) at least 25 feet apart.	Install emergency and normal power distribution systems (including electric panels, conduits, and switchgears) at least 50 feet apart.	A-11
Emergency Generator Protection	No special measures required.	If an emergency generator is used, secure it against unauthorized access.	If an emergency generator is used, secure against unauthorized access, and locate the emergency generator and fuel tank at least 25 feet away from loading docks, entrances, parking, or implement standoff, hardening and venting methods to protect utilities from the DBT at these locations.	If an emergency generator is used, secure against unauthorized access, and locate the emergency generator and fuel tank at least 25 feet away from loading docks, entrances, parking, or implement standoff, hardening, and venting methods to protect utilities from the DBT at these locations.	If an emergency generator is used, secure against unauthorized access, and locate the emergency generator and fuel tank at least 25 feet away from loading docks, entrances, parking, or implement standoff, hardening, and venting methods to protect utilities from the DBT at these locations.	A-11
Protection of Water Supply	No special measures required.	No special measures required.	Secure handles, control mechanisms, and service connections at on-site publicly-accessible locations with locks or other anti-tamper devices.	Secure handles, control mechanisms, and service connections at on-site publicly accessible locations with locks or other anti-tamper devices.	Secure handles, control mechanisms, and service connections at on-site publicly accessible locations with locks or other anti-tamper devices. Provide CCTV monitoring or periodic guard patrols.	A-12

STRUCTURE SECURITY CRITERIA

Aircraft as a Weapon	Arson	Assault	Ballistic Attack - Active Shooter	Ballistic Attack - Small Arms	Ballistic Attack - Standoff Weapons	Breach of Access Control Point - Covert	Breach of Access Control Point - Overt	CBR Release - External	CBR Release - Internal	CBR Release - Mailed or Delivered	CBR Release - Water Supply	Civil Disobedience	Disruption of Building & Security Systems	Explosive Device – Man-Portable External	Explosive Device – Man-Portable Internal	Explosive Device - Suicide/Homicide Bomber	Explosive Device – Vehicle Borne IED	Explosive Device - Mailed or Delivered	Hostile Surveillance	Kidnapping	Release of On-site Hazardous Materials	Robbery	Theft	Unauthorized Entry – Forced	Unauthorized Entry – Surreptitious	Vandalism	Vehicle Ramming	Workplace Violence
N	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
N	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
N	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
N	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
Y	Y	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	Y	Y	N
Y	Y	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	Y	Y	N
Y	Y	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	N	Y	Y	N	N	N	N	N	N	N	Y	Y	N
N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N

FACILITY ENTRANCE SECURITY CRITERIA

Security Criterion	Level I - Minimum	Level II - Low	Level III - Medium	Level IV - High	Level V - Very High	Details on Page
Badge Identification (ID) System	No special measures required.	Require agency photo ID that is worn and visible at all times when in government controlled space.	Require agency photo ID that is worn and visible at all times when in government controlled space.	Require agency photo ID that is worn and visible at all times when in government controlled space.	Require agency photo ID that is worn and visible at all times when in government controlled space.	A-13
Regulatory Signage	Post necessary regulatory, statutory, and/or site specific signage.	Post necessary regulatory, statutory, and/or site specific signage.	Post necessary regulatory, statutory, and/or site specific signage.	Post necessary regulatory, statutory, and/or site specific signage.	Post necessary regulatory, statutory, and/or site specific signage.	A-13
Employee Access Control	Issue employees keys for access.	Provide a means to secure employee entrance doors and to verify the identity of persons requesting access prior to allowing entry in the facility.	Provide a means to secure employee entrance doors. Require ID badge presentation to guards for visual and physical inspection before entry.	Provide a means to secure employee entrance doors. Require ID badge presentation to guards for visual and physical inspection before entry.	Provide a means to secure employee entrance doors. Require ID badge presentation to guards for visual and physical inspection before entry and for electronic authentication to allow entry.	A-13
Visitor Access Control	Entrances are open to the public during business hours. After hours, visitor entrances are secured, and have a means to verify the identity of persons requesting access prior to allowing entry into the facility.	Require visitors to nonpublic areas be sponsored by a tenant and either approved for unescorted access or escorted at all times.	Require visitors to nonpublic areas be sponsored by a tenant and either approved for unescorted access or escorted at all times. Require visitors to nonpublic areas display a visitor ID badge.	Require visitors to nonpublic areas be sponsored by a tenant and either approved for unescorted access or escorted at all times. Require visitors to nonpublic areas display a visitor ID badge.	Require visitors to nonpublic areas be sponsored by a tenant and either approved for unescorted access or escorted at all times. Require visitors to nonpublic areas display a visitor ID badge.	A-13
Occupant Screening	No special measures required.	No special measures required.	Use X-ray and magnetometer to screen all occupants and their property that do not possess an acceptable ID for access to the facility.	Use X-ray and magnetometer to screen all occupants and their property that do not possess an acceptable ID for access to the facility.	Use X-ray and magnetometer to screen all occupants and their property that do not possess an acceptable ID for access to the facility.	A-13
Visitor Screening	No special measures required.	No special measures required.	Screen all visitors and their property using X-ray and magnetometer.	Screen all visitors and their property using X-ray and magnetometer.	Screen all visitors and their property using X-ray and magnetometer.	A-13
Ballistic Protection at Screening Locations	No special measures required.	No special measures required.	No special measures required.	Provide a ballistic protective barrier in the utilization of guard booths, desks, or podiums where armed guards and other security personnel are stationed when interacting with unscreened personnel.	Provide a ballistic protective barrier in the utilization of guard booths, desks, or podiums where armed guards and other security personnel are stationed when interacting with unscreened personnel. Install ballistic-resistant doors and walls along the line of security screening.	A-13
Lobby Queuing	No special measures required.	No special measures required.	Minimize queuing caused by screening, visitor processing, and access control system throughput.	Minimize queuing caused by screening, visitor processing, and access control system throughput. Protect window and door glass in accordance with Blast Resistance for Windows in Critical and Vulnerable Areas.	Minimize queuing caused by screening, visitor processing, and access control system throughput. Protect window and door glass in accordance with Blast Resistance for Windows in Critical and Vulnerable Areas (page 50).	A-14

FACILITY ENTRANCE SECURITY CRITERIA

Aircraft as a Weapon	Arson	Assault	Ballistic Attack - Active Shooter	Ballistic Attack - Small Arms	Ballistic Attack - Standoff Weapons	Breach of Access Control Point - Covert	Breach of Access Control Point - Overt	CBR Release - External	CBR Release - Internal	CBR Release - Mailed or Delivered	CBR Release - Water Supply	Civil Disobedience	Disruption of Building & Security Systems	Explosive Device – Man-Portable External	Explosive Device – Man-Portable Internal	Explosive Device - Suicide/Homicide Bomber	Explosive Device – Vehicle Borne IED	Explosive Device - Mailed or Delivered	Hostile Surveillance	Kidnapping	Release of On-site Hazardous Materials	Robbery	Theft	Unauthorized Entry – Forced	Unauthorized Entry – Surreptitious	Vandalism	Vehicle Ramming	Workplace Violence
N	Y	Y	Y	N	N	Y	N	N	Y	N	N	N	Y	N	Y	N	N	N	Y	Y	Y	N	Y	N	Y	N	N	N
N	N	N	N	N	N	Y	N	N	Y	N	N	Y	N	N	Y	N	N	N	Y	N	Y	Y	Y	Y	Y	Y	N	Y
N	N	Y	Y	N	N	Y	Y	N	Y	N	N	N	Y	N	Y	N	N	N	Y	Y	Y	Y	Y	N	Y	N	N	Y
N	Y	Y	Y	N	N	Y	Y	N	Y	Y	N	Y	Y	N	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y	Y	N	N
N	N	N	Y	N	N	N	Y	N	Y	N	N	N	N	N	Y	N	N	N	Y	N	N	N	N	N	N	N	N	Y
N	N	Y	Y	N	N	Y	Y	N	Y	Y	N	Y	Y	N	Y	Y	N	Y	Y	Y	Y	Y	Y	N	Y	N	N	Y
N	N	Y	Y	Y	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N
N	N	Y	Y	Y	Y	Y	Y	N	Y	N	N	N	N	N	Y	Y	N	N	Y	Y	N	N	Y	N	Y	N	N	N

FACILITY ENTRANCE SECURITY CRITERIA

Security Criterion	Level I - Minimum	Level II - Low	Level III - Medium	Level IV - High	Level V - Very High	Details on Page
After Hours Access Control	No special measures required.	No special measures required.	Require all employees, contractors, and visitors to sign in and sign out electronically, or on a building register after-hours.	Require all employees, contractors, and visitors to sign in and sign out electronically, or on a building register after-hours.	Require all employees, contractors, and visitors to sign in and sign out electronically, or on a building register after-hours.	A-14
Limit Building Entry Points	No special measures required.	No special measures required.	Limit the number of building entry points to the fewest number practical.	Limit the number of building entry points to the fewest number practical.	Limit the number of building entry points to the fewest number practical.	A-14
Entrance Co-location	No special measures required.	No special measures required.	No special measures required.	Create separate flow patterns for employees and visitors at entrances.	Provide separate entrances for employees and visitors.	A-14
Perimeter Doors & Door Locks	Secure perimeter doors with high-security mechanical locks.	Secure perimeter doors with nonremovable hinges and high-security mechanical or electronic locks.	Secure perimeter doors with nonremovable hinges and high-security mechanical or electronic locks.	Secure perimeter doors with nonremovable hinges and high-security mechanical or electronic locks.	Secure perimeter doors with nonremovable hinges and high-security mechanical or electronic locks.	A-14
Control of Keys and Access Media	No special measures required.	Implement a formal key control program and electronically disable lost or stolen access media.	Implement a formal key control program and electronically disable lost or stolen access media.	Implement a formal key control program and electronically disable lost or stolen access media.	Implement a formal key control program and electronically disable lost or stolen access media.	A-14
Employee Convenience Doors	No special measures required.	No special measures required.	Provide electronic access control for employee entry doors without a guard post (including after-hours access) in conjunction with CCTV coverage.	Provide electronic access control for employee entry doors without a guard post (including after-hours access) in conjunction with CCTV coverage.	Provide electronic access control for employee entry doors without a guard post (including after-hours access) in conjunction with CCTV coverage.	A-15
Emergency Exit Doors	Secure emergency exit doors using an automatic door closer and exit hardware that are compliant with applicable life safety codes and standards.	Secure emergency exit doors using an automatic door closer and exit hardware that are compliant with applicable life safety codes and standards.	Secure emergency exit doors using an automatic door closer and exit hardware that are compliant with applicable life safety codes and standards.	Secure emergency exit doors using an automatic door closer and exit hardware that are compliant with applicable life safety codes and standards.	Secure emergency exit doors using an automatic door closer and exit hardware that are compliant with applicable life safety codes and standards.	A-15
Delayed Egress	No special measures required.	No special measures required.	No special measures required.	Use delayed egress hardware at emergency exits from critical or sensitive areas, if fire code allows.	Use delayed egress hardware at emergency exits from critical or sensitive areas, if fire code allows.	A-15

FACILITY ENTRANCE SECURITY CRITERIA

Aircraft as a Weapon	Arson	Assault	Ballistic Attack - Active Shooter	Ballistic Attack - Small Arms	Ballistic Attack - Standoff Weapons	Breach of Access Control Point - Covert	Breach of Access Control Point - Overt	CBR Release - External	CBR Release - Internal	CBR Release - Mailed or Delivered	CBR Release - Water Supply	Civil Disobedience	Disruption of Building & Security Systems	Explosive Device – Man-Portable External	Explosive Device – Man-Portable Internal	Explosive Device - Suicide/Homicide Bomber	Explosive Device – Vehicle Borne IED	Explosive Device - Mailed or Delivered	Hostile Surveillance	Kidnapping	Release of On-site Hazardous Materials	Robbery	Theft	Unauthorized Entry – Forced	Unauthorized Entry – Surreptitious	Vandalism	Vehicle Ramming	Workplace Violence
N	Y	N	Y	N	N	Y	Y	N	Y	Y	N	Y	Y	N	Y	N	N	Y	Y	Y	Y	N	Y	N	Y	Y	N	N
N	N	Y	Y	N	N	Y	Y	Y	Y	N	N	Y	N	N	Y	Y	N	N	Y	Y	Y	Y	Y	Y	Y	N	N	N
N	N	Y	Y	N	N	Y	Y	N	N	Y	N	N	N	N	N	Y	N	Y	Y	Y	N	N	N	N	N	N	N	Y
N	N	N	Y	N	N	Y	Y	N	Y	N	Y	Y	Y	N	N	N	N	N	Y	Y	Y	Y	Y	Y	Y	N	N	N
N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	Y	N	Y	Y	Y	N	Y	N	N	Y
N	N	N	Y	N	N	Y	Y	N	Y	N	N	Y	N	N	Y	Y	N	N	Y	Y	Y	Y	Y	Y	Y	Y	N	N
N	N	N	Y	N	N	Y	Y	N	Y	N	N	Y	N	N	Y	Y	N	N	Y	Y	Y	Y	Y	Y	Y	Y	N	N
N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	Y	N	N	N	N	N	N

INTERIOR SECURITY CRITERIA

Security Criterion	Level I - Minimum	Level II - Low	Level III - Medium	Level IV - High	Level V - Very High	Details on Page
Space Planning	No special measures required.	No special measures required.	Locate critical systems and areas at least 25 feet away from loading docks, entrances, mailrooms, personnel and package screening locations, and uncontrolled parking, or implement standoff, hardening, and venting methods to protect critical areas from the DBT at these locations.	Locate critical systems and areas at least 25 feet away from loading docks, entrances, mailrooms, personnel and package screening locations, and uncontrolled parking, or implement standoff, hardening, and venting methods to protect critical areas from the DBT at these locations.	Implement standoff, hardening, and venting methods to protect critical areas from the DBT at loading docks, entrances, mailrooms, personnel and package screening locations, and uncontrolled parking.	A-16
Access to nonpublic Areas	Use signage to designate nonpublic areas and establish procedures to prevent unauthorized access.	Use signage to designate nonpublic areas and establish procedures to prevent unauthorized access.	Use signage, stanchions, counters, furniture, knee walls, etc., to establish physical boundaries to control access to nonpublic areas.	Use signage, walls, IDS, and electronic access control and/or security guards to establish physical boundaries to control access to nonpublic areas.	Use signage, walls, IDS, and electronic access control and/or security guards to establish physical boundaries to control access to nonpublic areas.	A-16
Security of Critical Areas	Lock doors to critical areas and establish procedures to limit access into critical areas to authorized personnel only.	Lock doors to critical areas and establish procedures to limit access into critical areas to authorized personnel only.	Install electronic access control and IDS to control and monitor access into critical areas.	Install electronic access control and IDS to control and monitor access into critical areas.	Install electronic access control and IDS to control and monitor access into critical areas.	A-16
Building Systems and Roof Access	Secure utility, mechanical, electrical, and telecom rooms, and access to interior space from the roof with locks.	Secure utility, mechanical, electrical, and telecom rooms, and access to interior space from the roof with high-security locks.	Secure utility, mechanical, electrical, and telecom rooms, and access to interior space from the roof using locks and IDS.	Secure utility, mechanical, electrical, and telecom rooms, and access to interior space from the roof using electronic access control and IDS.	Secure utility, mechanical, electrical, and telecom rooms, and access to interior space from the roof using electronic access control, IDS, and CCTV monitoring.	A-16
Publicly Accessible Restrooms	Control access to public restrooms.	Control access to public restrooms.	Screen the public before accessing restrooms.	Screen the public before accessing restrooms.	Deny public access to restrooms.	A-16
Publicly Accessible Retail and Mixed Use Space	No special measures required.	Accommodate publiclyaccessible retail and mixed uses through such means as separating entryways.	Accommodate publiclyaccessible retail and mixed uses through such means as separating entryways.	Accommodate publiclyaccessible retail and mixed uses through such means as controlling access, screening, and guards.	Prohibit publiclyaccessible retail and mixed use space.	A-16
Blast Resistance - Interior Public Spaces	No special measures required	Use construction materials which have inherent ductility and which are better able to respond to load reversals (e.g., cast in place reinforced concrete column construction).	Implement architectural or structural features, or other positive countermeasures that deny contact with exposed primary vertical load members in these areas. A minimum standoff of at least 100 mm (4 inches) is required.	Utilize hardening and venting methods to prevent progressive collapse and limit airblast injuries in adjacent areas from the DBT in an area accessible to unscreened persons. Significant structural damage to the walls, ceilings, and floors of the public area may occur, however, the adjacent areas should not experience severe damage or collapse.	Utilize hardening and venting methods to prevent progressive collapse and limit airblast injuries in adjacent areas from the DBT in an area accessible to unscreened persons. Significant structural damage to the walls, ceilings, and floors of the public area may occur, however, the adjacent areas should not experience severe damage or collapse.	A-17

INTERIOR SECURITY CRITERIA

INTERIOR SECURITY CRITERIA

Security Criterion	Level I - Minimum	Level II - Low	Level III - Medium	Level IV - High	Level V - Very High	Details on Page
Blast Resistance - Mail Screening and Receiving Location	No special measures required	Use construction materials in the mail screening and receiving areas which have inherent ductility and which are better able to respond to load reversals (e.g., cast in place reinforced concrete column construction).	Implement architectural or structural features, or other positive countermeasures in the mail screening and receiving areas that deny contact with exposed primary vertical load members and/or lateral bracing members in these areas. A minimum standoff of at least 150 mm (6 inches) is required.	Utilize hardening and venting methods to prevent progressive collapse and limit airblast injuries in adjacent areas from the DBT in a mail screening or receiving area. Significant structural damage to the walls, ceilings, and floors of the mailroom/receiving area may occur. However, the adjacent areas should not experience severe damage or collapse.	Utilize hardening and venting methods to prevent progressive collapse and limit airblast injuries in adjacent areas from the DBT in a mail screening or receiving area. Significant structural damage to the walls, ceilings, and floors of the mailroom/receiving area may occur. However, the adjacent areas should not experience severe damage or collapse.	A-17
Interior Windows	No special measures required.	No special measures required.	No special measures required.	Provide tempered or high-strength glass.	Provide tempered or high-strength glass.	A-17

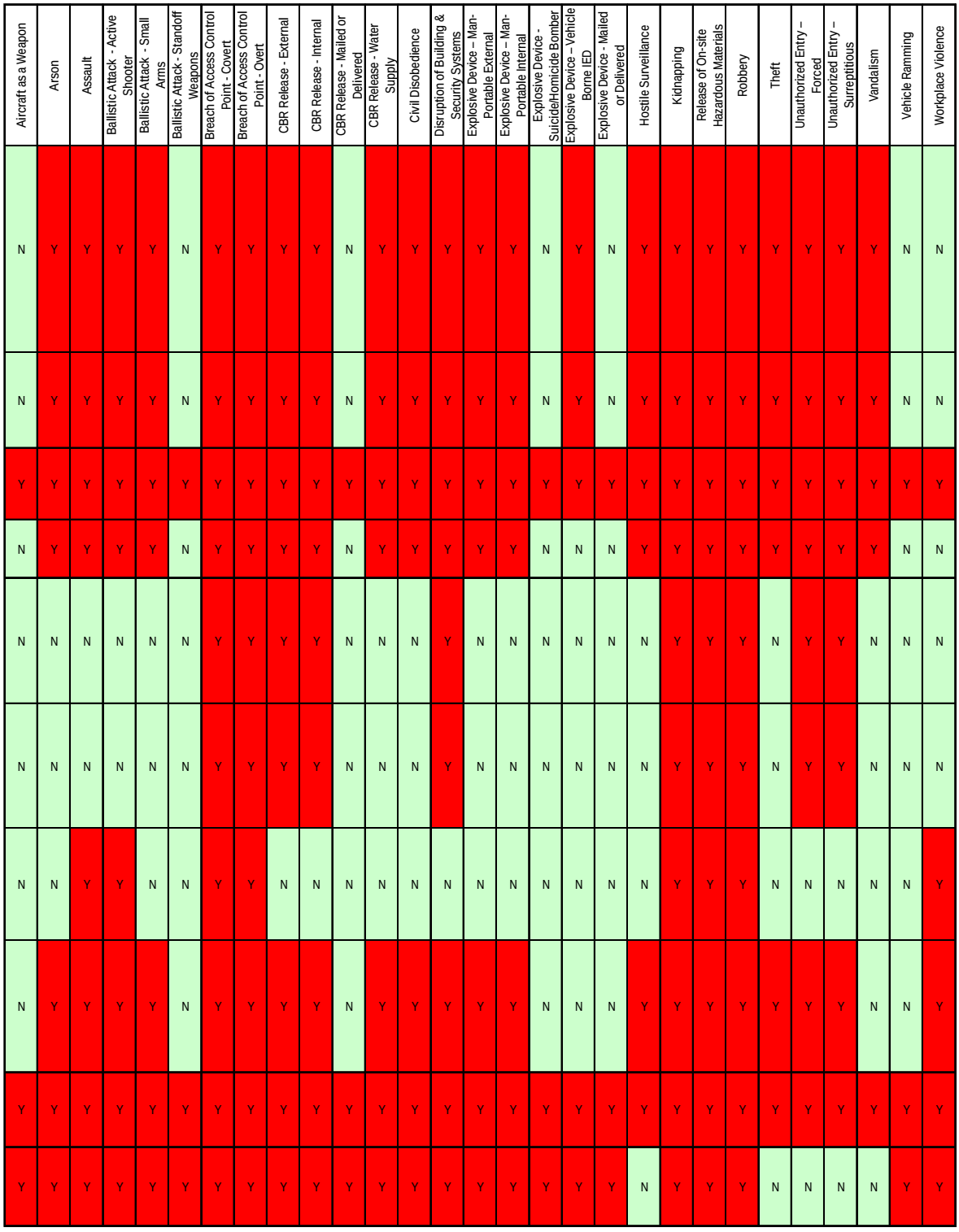
INTERIOR SECURITY CRITERIA

Aircraft as a Weapon	Arson	Assault	Ballistic Attack - Active Shooter	Ballistic Attack - Small Arms	Ballistic Attack - Standoff Weapons	Breach of Access Control Point - Covert	Breach of Access Control Point - Overt	CBR Release - External	CBR Release - Internal	CBR Release - Mailed or Delivered	CBR Release - Water Supply	Civil Disobedience	Disruption of Building & Security Systems	Explosive Device – Man-Portable External	Explosive Device – Man-Portable Internal	Explosive Device - Suicide/Homicide Bomber	Explosive Device – Vehicle Borne IED	Explosive Device - Mailed or Delivered	Hostile Surveillance	Kidnapping	Release of On-site Hazardous Materials	Robbery	Theft	Unauthorized Entry – Forced	Unauthorized Entry – Surreptitious	Vandalism	Vehicle Ramming	Workplace Violence
N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N
N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N

SECURITY SYSTEMS CRITERIA

Security Criterion	Level I - Minimum	Level II - Low	Level III - Medium	Level IV - High	Level V - Very High	Details on Page
CCTV Coverage	No special measures required.	Provide CCTV coverage of pedestrian entrances and exits.	Provide CCTV coverage of screening checkpoints, pedestrian and vehicle entrances, exits, loading docks, and lobbies.	Provide CCTV coverage of screening checkpoints, exits, loading docks, lobbies, facility perimeter, parking areas, sensitive interior areas, pedestrian and vehicle entrances, and other potential access points.	Provide CCTV coverage of screening checkpoints, pedestrian and vehicle entrances, exits, loading docks, lobbies, facility perimeter, parking areas, sensitive interior areas, other potential access points, and potential criminal and terrorist pre-operational surveillance locations.	A-18
CCTV Monitoring and Recording	No special measures required.	Record CCTV views using time-lapse video recording.	Record CCTV views using time-lapse video recording and digital image storage.	Provide alarm-activated CCTV monitoring and recording using time-lapse video and digital image storage.	Conduct active CCTV monitoring and recording using time-lapse video and digital image storage.	A-18
Security Control Center	No special measures required.	No special measures required.	No special measures required.	Provide an onsite central security control center, staffed during operating hours.	Provide an onsite central security control center, staffed 24/7.	A-19
CCTV Surveillance Advisory	Post signage advising of CCTV surveillance when required.	Post signage advising of CCTV surveillance when required.	Post signage advising of CCTV surveillance when required.	Post signage advising of CCTV surveillance when required.	Post signage advising of CCTV surveillance when required.	A-19
Intrusion Detection System (IDS) Coverage	No special measures required.	Provide IDS on perimeter entry and exit doors, and operable ground-floor windows.	Provide IDS on perimeter entry and exit doors, and all ground-floor windows.	Provide IDS on perimeter entry and exit doors, and all windows within 16 feet of the ground or other access point.	Provide IDS on perimeter entry and exit doors, all windows within 16 feet of the ground or other access point, and any other openings larger than 96 square inches.	A-20
Intrusion Detection System (IDS) Monitoring	Install local annunciation if IDS is in use.	Monitor at a central station with notification to a building manager or designated tenant POC.	Monitor at a central station (onsite or offsite) with notification to law enforcement or security responders.	Monitor at an on-site central station during operating hours, and offsite after hours, with response by law enforcement or security responders.	Monitor at an on-site central station with response by on-site guard-force.	A-20
Duress Alarms or Assistance Stations	Implement duress procedures for emergency situations.	Implement duress procedures for emergency situations.	Provide duress buttons or call buttons at guard posts and sensitive public contact areas.	Provide duress buttons or call buttons at guard posts, sensitive public contact areas, in garages, and other areas that are identified as high-risk locations.	Provide duress buttons or call buttons at guard posts, sensitive public contact areas, in garages, and other areas that are identified as high-risk locations.	A-21
Security System Integrity	No special measures required.	No special measures required.	No special measures required.	Secure alarm and physical access control panels, CCTV components, controllers, and cabling against unauthorized access.	Secure alarm and physical access control panels, CCTV components, controllers, and cabling against unauthorized access. Utilize supervised circuits for alarms.	A-21
Security Communications	No special measures required.	No special measures required.	No special measures required.	Provide a centralized radio network for guard-force personnel.	Provide a centralized, secure and monitored radio network for guard-force personnel.	A-21
Building Communication System	No special measures required.	No special measures required.	Provide a communication system for security and emergency announcements.	Provide a communication system for security and emergency announcements.	Provide a communication system for security and emergency announcements.	A-21

SECURITY SYSTEMS CRITERIA



SECURITY SYSTEMS CRITERIA

Security Criterion	Level I - Minimum	Level II - Low	Level III - Medium	Level IV - High	Level V - Very High	Details on Page
Emergency Power for Security Systems	No special measures required.	No special measures required.	Provide uninterruptible emergency power to essential electronic security systems for a minimum of 4 hours.	Provide uninterruptible emergency power to essential electronic security systems for a minimum of 4 hours.	Provide uninterruptible emergency power to essential electronic security systems for as long as mission requirements dictate continuous operation of the facility.	A-21
Security System Testing	No special measures required.	Conduct security system performance testing annually.	Conduct security system performance testing annually.	Conduct security system performance testing annually.	Conduct security system performance testing annually.	A-21
Security System Maintenance	No special measures required.	Implement a preventive maintenance program for all security systems. Any critical component that becomes inoperable must be replaced or repaired within five business days.	Implement a preventive maintenance program for all security systems. Any critical component that becomes inoperable must be replaced or repaired within 72 hours.	Implement a preventive maintenance program for all security systems. Any critical component becomes inoperable for service must be replaced or repaired within five business days.	Implement a preventive maintenance program for all security systems. Any critical component becomes inoperable for service must be replaced or repaired within five business days.	A-22

SECURITY SYSTEMS CRITERIA

Aircraft as a Weapon	Arson	Assault	Ballistic Attack - Active Shooter	Ballistic Attack - Small Arms	Ballistic Attack - Standoff Weapons	Breach of Access Control Point - Covert	Breach of Access Control Point - Overt	CBR Release - External	CBR Release - Internal	CBR Release - Mailed or Delivered	CBR Release - Water Supply	Civil Disobedience	Disruption of Building & Security Systems	Explosive Device – Man-Portable External	Explosive Device – Man-Portable Internal	Explosive Device - Suicide/Homicide Bomber	Explosive Device – Vehicle Borne IED	Explosive Device - Mailed or Delivered	Hostile Surveillance	Kidnapping	Release of On-site Hazardous Materials	Robbery	Theft	Unauthorized Entry – Forced	Unauthorized Entry – Surreptitious	Vandalism	Vehicle Ramming	Workplace Violence
N	Y	Y	Y	Y	N	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	Y	N	Y	Y	Y	Y	Y	Y	Y	N	N	Y
N	Y	Y	Y	Y	N	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y	Y	Y	Y	Y	N	N	Y
N	Y	Y	Y	Y	N	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	N	N	N	Y	Y	Y	Y	Y	Y	Y	N	N	Y

SECURITY OPERATIONS AND ADMINISTRATION CRITERIA

Security Criterion	Level I - Minimum	Level II - Low	Level III - Medium	Level IV - High	Level V - Very High	Details on Page
Designated Official (DO)	Identify the DO who is responsible for security, safety, and emergency management in the facility.	Identify the DO who is responsible for security, safety, and emergency management in the facility.	Identify the DO who is responsible for security, safety, and emergency management in the facility.	Identify the DO who is responsible for security, safety, and emergency management in the facility.	Identify the DO who is responsible for security, safety, and emergency management in the facility.	A-23
Facility Security Committee (FSC)	Establish an FSC that is chaired by the DO (or designee) to provide oversight of security, life-safety, and emergency procedures.	Establish an FSC that is chaired by the DO (or designee) to provide oversight of security, life-safety, and emergency procedures.	Establish an FSC that is chaired by the DO (or designee) to provide oversight of security, life-safety, and emergency procedures.	Establish an FSC that is chaired by the DO (or designee) to provide oversight of security, life-safety, and emergency procedures.	Establish an FSC that is chaired by the DO (or designee) to provide oversight of security, life-safety, and emergency procedures.	A-23
Security Operations Management	No special measures required.	No special measures required.	Provide a federal security manager with oversight responsibilities for guards and other physical security operations who is onsite at least weekly.	Provide a federal security manager with oversight responsibilities for guards and other physical security operations who is onsite at least daily.	Provide a federal security manager with oversight responsibilities for guards and other physical security operations who is onsite 24/7.	A-23
Guard Fixed Post - Exterior	No special measures required.	No special measures required.	No special measures required.	No special measures required.	Provide fixed guard posts on exterior to challenge and identify approaching persons prior to entry into the building 24/7.	A-23
Guard Fixed Posts - Screening Checkpoints	No special measures required.	No special measures required.	Post armed guards at all screening checkpoints.	Post armed guards at all screening checkpoints.	Post armed guards at all screening checkpoints.	A-23
Guard Patrols	No special measures required.	No special measures required.	No special measures required.	Establish hourly interior and exterior roving armed guard patrols during normal business hours.	Establish hourly interior and exterior roving armed guard patrols 24/7.	A-23
Guard Response	No special measures required.	No special measures required.	Develop plans for on-site security guard response to alarms and incidents.	Develop plans for on-site security guard response to alarms and incidents.	Develop plans for on-site security guard response to alarms and incidents.	A-23
Facility Security Plan	Develop a written facility security plan that identifies security responsibilities, emergency contacts, response procedures for incidents, and contingency plans for temporary upgrades in accordance with the Homeland Security Advisory System.	Develop a written facility security plan that identifies security responsibilities, emergency contacts, response procedures for incidents, and contingency plans for temporary upgrades in accordance with the Homeland Security Advisory System.	Develop a written facility security plan that identifies security responsibilities, emergency contacts, response procedures for incidents, and contingency plans for temporary upgrades in accordance with the Homeland Security Advisory System.	Develop a written facility security plan that identifies security responsibilities, emergency contacts, response procedures for incidents, and contingency plans for temporary upgrades in accordance with the Homeland Security Advisory System.	Develop a written facility security plan that identifies security responsibilities, emergency contacts, response procedures for incidents, and contingency plans for temporary upgrades in accordance with the Homeland Security Advisory System.	A-24
Occupant Emergency Plan (OEP)	Develop, publish, and maintain an OEP, and conduct annual training/exercises.	Develop, publish, and maintain an OEP, and conduct annual training/exercises.	Develop, publish, and maintain an OEP, and conduct annual training/exercises.	Develop, publish, and maintain an OEP, and conduct annual training/exercises.	Develop, publish, and maintain an OEP, and conduct annual training/exercises.	A-24
Availability of Emergency Plans and Documents	Ensure ready availability of emergency plans and associated documents in the event of an emergency.	Ensure ready availability of emergency plans and associated documents in the event of an emergency.	Ensure ready availability of emergency plans and associated documents in the event of an emergency.	Ensure ready availability of emergency plans and associated documents in the event of an emergency.	Ensure ready availability of emergency plans and associated documents in the event of an emergency.	A-24
Protection of Construction Information	No special measures required.	No special measures required.	Limit access to construction documents to those persons with an established need-to-know.	Limit access to construction documents to those persons with an established need-to-know.	Limit access to construction documents to those persons with an established need-to-know.	A-25
Security During Construction and Renovation	No special measures required.	Develop and implement a Construction Security Plan.	Develop and implement a Construction Security Plan.	Develop and implement a Construction Security Plan.	Develop and implement a Construction Security Plan.	A-25

SECURITY OPERATIONS AND ADMINISTRATION CRITERIA

Aircraft as a Weapon	Arson	Assault	Ballistic Attack - Active Shooter	Ballistic Attack - Small Arms	Ballistic Attack - Standoff Weapons	Breach of Access Control Point - Covert	Breach of Access Control Point - Overt	CBR Release - External	CBR Release - Internal	CBR Release - Mailed or Delivered	CBR Release - Water Supply	Civil Disobedience	Disruption of Building & Security Systems	Explosive Device – Man-Portable External	Explosive Device – Man-Portable Internal	Explosive Device - Suicide/Homicide Bomber	Explosive Device – Vehicle Borne IED	Explosive Device - Mailed or Delivered	Hostile Surveillance	Kidnapping	Release of On-site Hazardous Materials	Robbery	Theft	Unauthorized Entry – Forced	Unauthorized Entry – Surreptitious	Vandalism	Vehicle Ramming	Workplace Violence
Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	Y	Y
Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
N	Y	Y	Y	Y	N	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	N	N	Y	Y	N	Y	Y	Y	Y	Y	N	N
N	N	Y	Y	N	N	N	Y	N	N	N	N	Y	N	N	Y	Y	N	N	N	Y	N	Y	N	N	N	N	N	Y
N	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	N	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y	Y	N	N
Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	N	Y	Y
Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	N	N	N	Y	Y
Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	Y	N
N	N	N	N	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	N	Y	Y	Y	N	Y	N	N	Y	Y	N	N	N
N	Y	Y	N	N	N	Y	N	N	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N	Y	N	Y	Y	Y	Y	N	N

SECURITY OPERATIONS AND ADMINISTRATION CRITERIA

Security Criterion	Level I - Minimum	Level II - Low	Level III - Medium	Level IV - High	Level V - Very High	Details on Page
Mail/Package Handling and Other Deliveries	Follow ISC Safe Mail Handling Procedures.	Inspect all mail/packages and deliveries visually prior to distribution throughout the facility.	Screen all mail and packages using X-ray at a loading dock if present or at an existing screening location if there is no loading dock. Physically inspect items that cannot be passed through screening equipment.	Screen all mail and packages using X-ray in a dedicated mail receiving facility located away from facility main entrances, areas containing critical services, utilities, distribution systems, and important assets. Install an outside wall, door, or window designed to relieve blast pressures. Physically inspect items that cannot be passed through screening equipment.	Screen all mail and packages using X-ray in isolated, external, or off-site mail receiving facility consistent with ISC Safe Mail Handling Procedures. Physically inspect items that cannot be passed through screening equipment.	A-26
Security Awareness Training	Provide all employees with annual security awareness training.	Provide all employees with annual security awareness training.	Provide all employees with annual security awareness training.	Provide all employees with annual security awareness training.	Provide all employees with annual security awareness training.	A-26

SECURITY OPERATIONS AND ADMINISTRATION CRITERIA

Aircraft as a Weapon	Arson	Assault	Ballistic Attack - Active Shooter	Ballistic Attack - Small Arms	Ballistic Attack - Standoff Weapons	Breach of Access Control Point - Covert	Breach of Access Control Point - Overt	CBR Release - External	CBR Release - Internal	CBR Release - Mailed or Delivered	CBR Release - Water Supply	Civil Disobedience	Disruption of Building & Security Systems	Explosive Device – Man-Portable External	Explosive Device – Man-Portable Internal	Explosive Device - Suicide/Homicide Bomber	Explosive Device – Vehicle Borne IED	Explosive Device - Mailed or Delivered	Hostile Surveillance	Kidnapping	Release of On-site Hazardous Materials	Robbery	Theft	Unauthorized Entry – Forced	Unauthorized Entry – Surreptitious	Vandalism	Vehicle Ramming	Workplace Violence
N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N
Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y

Undesirable Events

The table below defines the context of the undesirable events against which each criterion is matched. The descriptions are not legal definitions; rather, they are offered to establish a conceptual scenario for use in identifying applicable countermeasures when applying this Standard.

Additional information on each undesirable event, including specific capabilities or methods, an assessment of the level of threat, and factors which may influence the threat to a particular facility are available in the ISC DBT document.

Undesirable Event	Description
Aircraft as a Weapon	Attack on a facility using an aircraft as an improvised explosive device.
Arson	An attack against a Government facility by knowingly and willingly setting a fire with the intent to cause damage or destruction to the facility and/or physical injury or loss of life to the occupants.
Assault	Physically assaulting (with or without a weapon) a building occupant or visitor inside the facility or on the property.
Ballistic Attack - Active Shooter	Movement of an adversary(s) through a facility and discriminately and/or indiscriminately engaging occupants and visitors with gunfire.
Ballistic Attack - Small Arms	Firearm fired from offsite into a facility or a defined area.
Ballistic Attack - Standoff Weapons	Mortar, rocket-propelled grenade, etc., fired from offsite into a facility or area.
Breach of Access Control Point - Covert	Use of deceit, coercion, or social engineering to gain access to a facility through a controlled entrance.
Breach of Access Control Point - Overt	The use of force and/or weapons to defeat a personnel screening or access control checkpoint (including ID checks).
CBR Release - External	Dispersal of a CBR agent in a general area affecting personnel or buildings in the area or through a specific access point (e.g., air intakes, windows, or doorways) from outside the facility.
CBR Release - Internal	Intentional release of a CBR agent carried into the facility, including in general interior spaces (lobbies) or into specific rooms or systems (HVAC rooms).
CBR Release - Mailed or Delivered	A CBR substance or dispersal device sent to the facility through U.S. Mail or a commercial delivery service, including an unwitting courier.
CBR Release - Water Supply	Introduction of a CBR agent into the water supply for a specific facility from outside the facility.
Civil Disobedience	Generic discussion of how demonstrations can devolve into any of the singular undesirable events.
Disruption of Building & Security Systems	Physically accessing building or security systems for the purposes of disruption or manipulation of the systems. (Does not include cyber attacks. Prevention of cyber attacks is outside the scope of this document).
Explosive Device – Man-Portable External	An explosive device planted on the property but outside of a building and left to detonate after the adversary departs.
Explosive Device – Man-Portable Internal	An explosive device carried into the building by an adversary or an unwitting occupant or visitor, and left to detonate after the adversary departs.

Undesirable Event	Description
Explosive Device - Suicide/Homicide Bomber	An explosive device carried into the building by an adversary with the intent of reaching a specific target or area, and detonating the device.
Explosive Device – Vehicle Borne IED	Placement of an explosive device in a vehicle, which is then positioned in a vulnerable location with respect to the facility and detonated.
Explosive Device - Mailed or Delivered	An explosive device sent to the facility through U.S. Mail or a commercial delivery service, including an unwitting courier.
Hostile Surveillance	Conducting surveillance of key assets, personnel, security features, operations, or sensitive areas from offsite or outside secure areas for the purposes of collection of information in preparation for an attack.
Kidnapping	Abduction of an occupant or visitor from a facility, including from inside secured areas (e.g., a daycare center) or outside on the site (e.g., a Government-controlled parking lot).
Release of On-site Hazardous Materials	Unauthorized access to hazardous materials stored onsite with the intent of harming personnel or damaging the facility.
Robbery	Unauthorized removal of Government-owned or personal property from an occupant or visitor by force or threat of force.
Theft	Unauthorized removal of Government-owned or personal property from a facility.
Unauthorized Entry – Forced	Unauthorized access to a facility or controlled area by forced entry.
Unauthorized Entry – Surreptitious	Unauthorized access to a facility or controlled area by stealth.
Vandalism	Destruction, damage, or defacing of Government-owned or personal property or assets.
Vehicle Ramming	Driving a vehicle in an attempt to penetrate a facility (e.g., lobby or loading dock) or breach a defined perimeter.
Workplace Violence	Violence perpetrated by an occupant (or former occupant) on another within a facility.

This Page Intentionally Left Blank

Appendix A – Details of Security Measures

Effective deployment of countermeasures requires a full understanding of the recommended security measure. Accordingly, the tables below give details of selected security measures identified in Section 7.0. As in that section, criteria are grouped according to site, structure, facility entrances, interior, security systems, and operations and administration. This additional detail is provided to convey the full meaning and scope of those baseline security measures whose title and brief description alone are not sufficient. For those measures for which additional detail is not provided, the baseline description is considered sufficient.

This Page Intentionally Left Blank

Index of Details of Security Measures

Site

Security Criterion	Detail	Criteria Page
Identification as Federal Facility	Where the interaction with visitors is customer-service oriented, such as Social Security Administration customer service centers, Veterans Administration hospitals, etc., and signage would improve the ability of customers to locate the facility, use of external signage would be appropriate. Agencies who routinely contact or attract the attention of dangerous groups capable or with stated intent to cause direct harm (FBI, ATF, DEA, CIA, DHS) should avoid the use of external identifying signage when possible.	46
Landscaping	Landscaping may be used as a protective measure to obstruct views from outside a facility or as a physical barrier. A balance must be achieved between its usefulness in protection and its potential negative impact on security measures. Apply principles of Crime Prevention Through Environmental Design (CPTED) where appropriate. CPTED is a crime prevention strategy that uses architectural design, landscape planning, security systems and visual surveillance to create a potentially crime-free environment by influencing human behavior. CPTED usually involves the use of four principles: (1) Natural Surveillance (by placing physical features, activities, lighting, and people to preclude bind spots or hiding spots to keep intruders easily observable); (2) Territorial Reinforcement (using buildings, fences, different paving material, changes in street elevation, signs, and other landscaping to express ownership by distinguishing to potential offenders private spaces from public spaces), (3) Natural Access Control (strategic placement of entrances, exits, fencing, landscaping, and lighting to create in potential offenders a perception of risk); and (4)Target Hardening (use of features that prohibit entry or access, such as perimeter boulders/large rocks, streetscape furniture, art ornaments, etc.).	46
Pedestrian Access to Site	The level of protection afforded by the barriers should be commensurate with the need to limit pedestrian access. Higher levels of protection, intended to prevent determined intruders, are achieved using anti-climb fences or razor/barbed wire. Lower levels of protection, intended to guide pedestrians, can be achieved using shrubbery, decorative fencing, or knee walls.	46
Vehicle Access Points	Reducing the number of vehicle access points, particularly under periods of heightened threat, reduces vulnerability and security costs associated with monitoring and controlling access to the site.	46

Security Criterion	Detail	Criteria Page
Site Lighting	For minimum lighting levels, refer to the Illuminating Engineering Society (IES) Lighting Handbook. Lighting should be sufficient to illuminate potential areas of concealment, enhance the observation of guard patrols, and provide for the safety of personnel moving between adjacent parking areas, streets, alleyways, and around the facility. Site lighting should be coordinated with the closed-circuit television (CCTV) system. Maintained Illumination Level (lux) Horizontal Illumination - Covered parking areas - 10 - Roof and surface parking area - 2.5 - Stairwells, elevator lobbies - 20 - Uniformity ratio (average:min) 4:1 - Uniformity ratio (maximum:min) 20:1 Vertical Illumination - Covered parking areas-5 - Roof and surface parking area-2.5 - Stairwells, elevator lobbies-10 Consider using motion detection where appropriate.	46
Restricted Areas	Restricted areas include but are not limited to utility connections, loading docks, emergency power supplies, child-care play yards, hazardous-materials storage, HVAC, and exterior access to critical rooms such as telecom and IT resources. Transparency or opaqueness and height of the fence is a site-specific determination. The level of protection afforded by the barriers should be commensurate with the need to limit pedestrian access. Higher levels of protection, intended to prevent determined intruders, are achieved using anti-climb fences or razor/barbed wire. Lower levels of protection, intended to guide pedestrians, can be achieved using shrubbery, decorative fencing, or knee walls.	46
Signage - Sensitive Areas	Avoid marking outside locations such as air intakes, fuel supply valves, gas or power distribution locations, evacuation assembly areas, etc.	46
Control of Parking	Government control of parking, or other formal arrangements with the owner of non-Government parking, is required to ensure the limitation of parking to authorized vehicles. Post "No Parking" signage and arrange for towing of unauthorized vehicles where parking is restricted. For the Level V - Very High LOP, the setback distance is determined as part of determining the LOP (a combination of hardening and setback to defeat the DBT) to "Blast Protection - Windows," "Blast Protection - Façade," and "Blast Resistance - Progressive Collapse." All parking within that setback distance must be controlled.	46
Authorized Parking	Utilize a parking pass or other similar system to clearly identify authorized vehicles upon entry and while parked. Passes should be visible, numbered, have an expiration date, and issuance should be managed by a single authority. Visitor parking should be located as far from the facility as practical. Assigned employee and Government parking may be used to establish a "buffer zone."	46

Security Criterion	Detail	Criteria Page
Vehicle Access to Controlled Parking	Reference the DBT document for vehicle size and type. Use a vehicle velocity that considers the angle of incidence in conjunction with the distance between the perimeter and the point at which a vehicle likely would be able to start a run at the perimeter. Design site circulation to prevent high-speed approaches by vehicles, and use barriers or offset vehicle entrances from the direction of a vehicle's approach to force a reduction in speed.	48
Vehicle Barriers	Reference the DBT document for vehicle size and type. Use a vehicle velocity that considers the angle of incidence in conjunction with the distance between the perimeter and the point at which a vehicle likely would be able to start a run at the perimeter. Design site circulation to prevent high speed approaches by vehicles, and use barriers or offset vehicle entrances from the direction of a vehicle's approach to force a reduction in speed. Appropriate measures for the barrier system may include walls, fences, trenches, berms, ponds and water basins, boulders, plantings, trees, static barriers, sculptures, and street furniture. Maximum clear spacing between vehicle barriers is 4 feet. Minimum barrier height is 30 inches. Barriers must be certified to meet performance requirements for vehicle size and speed specific to the facility under ASTM F 2656, Standard Test Method for Vehicle Crash Testing of Perimeter Barriers, or SD-STD-02.01, Revision A, Test Method for Vehicle Crash Testing of Perimeter Barriers and Gates.	48
Vehicle Screening	At a minimum, vehicle screening should include a visual inspection of the vehicle exterior, undercarriage, passenger compartment, and trunk. For higher risk facilities, consider explosive trace detection systems or canine support. Provide adequate lighting in screening area to illuminate the vehicle exterior and undercarriage. Provide CCTV coverage of the screening area. Use barrier systems to ensure vehicles cannot pass beyond the screening checkpoint until cleared. Site configuration permitting, vehicle inspection areas should be located beyond the setback distance. The setback distance is determined as part of determining the LOP (a combination of hardening and setback to defeat the DBT) to "Blast Protection - Windows," "Blast Protection - Façade," and "Blast Resistance - Progressive Collapse." All parking within that setback distance must be controlled.	48

Security Criterion	Detail	Criteria Page
Pedestrian Access to Controlled Parking Areas	Limit the number of entrances to the extent practicable. Monitoring of parking areas can be accomplished with CCTV, guard patrols, or visually from fixed security posts. At a minimum, pedestrian barriers around parking areas should be designed to prevent casual access and increase the visibility of unauthorized access attempts. In higher risk applications, anti-climb fences, etc., may be used to defeat attempts to cross over the barrier. When required, positive access control may be achieved using electronic access control systems or security checkpoints.	48
Hazardous Materials Storage	Comply with applicable regulations regarding storage and safety requirements. Depending on the nature of the HAZMAT, measures may need to be designed to prevent access to, release of, or unauthorized removal of the HAZMAT from the site. Valves and control mechanisms also must be protected from unauthorized access.	48
Receptacle and Container Placement	All areas of potential concealment for IEDs should be routinely examined by security patrols. Ensure that containers can be removed during periods of heightened alert. Blast-mitigating containers should be designed to defeat the DBT device. Reference the DBT document for device size and type.	48

Structure

Security Criterion	Detail	Criteria Page
Blast Resistance - Windows	Reference the current DBT established by the ISC, unless device size is superseded by an agency-specific threat assessment. Device location is the closest possible point to the protected setback with the DBT device. In high and very high LOP, the window system shall be of balanced design where the glazing will fail prior to the window framing and anchorage, or the windows and window frame and anchorage shall meet the specified performance condition up to the DBT bomb loading. Windows in doors shall meet the same specification as the windows in the building or not fail before the door under blast loadings. Where peak pressures from the DBT can be shown to be below 1 psi acting on the face of the building, you may use the reduced requirements of installing acceptable or preferred glazing systems. Due to high air blast pressures in close proximity to the DBT, it is not always feasible to fully meet the blast requirements for high and very high levels of protection for all of the windows on a building. While 100% is desired, a common goal is to have 90% of the glazing in the facility fully meet the performance. Preferred glazing systems include: thermally tempered heat strengthened or annealed glass with a fragment retention film installed on the interior surface and attached to the frame; laminated thermally tempered, laminated heat strengthened, or laminated annealed glass. Acceptable glazing systems include thermally tempered glass; and thermally tempered, heat strengthened or annealed glass with fragment retention film installed on the interior surface (edge to edge, wet glazed, or daylight installations are acceptable). In some cases, a combination of one of these preferred or acceptable systems and a catchment system (blast curtains, blast blinds, catch rods, etc.) may be effective, particularly when pressures above the designed strength are possible. Catchment systems should generally not be used alone, but blast curtains in particular are an acceptable alternative for situations where building conditions prohibit application of fragment retention film. Blast curtain catchment systems are acceptable for performance condition 3b, provided they have been certified as meeting the US General Services Administration Standard Test Method for Glazing and Window Systems Subject to Dynamic Overpressure Loadings (intended to ensure the resistance of the material to penetration and failure); and, they are engineered or tested for the actual application so as to limit "billowing" of the curtain system and fragment penetration to the maximum 10-foot limit. The design of some catchment systems permits occupants to pull them aside or gather them together in the middle of a window, reducing their effectiveness. Operational measures may be required to prevent this. Unacceptable systems include untreated monolithic annealed or heat strengthened glass; and wire glass. New glazing systems at the Low or higher LOP shall be designed with a minimum ½-inch bite. All glazing hazard reduction products for High and Very High LOP require product specific test results and engineering analyses performed by qualified independent agents demonstrating the performance of the product under the specified blast loads, and stating that it meets or exceeds the minimum performance required in the figure below. The glazing hazard reduction product shall all also be shown by testing, calculations, or interpolation as approved by the agency to meet the performance required for the actual window sizes in the building. For new construction projects and major rehabilitation projects over 100,000 GSF, a blast engineer with formal training in structural dynamics, and demonstrated experience with accepted design practices for blast resistant design must be included as a member of the design team. In applications requiring retention film, acceptable fragment retention film shall be meet or exceed the following physical properties: - Film composite strength and elongation rate measured at a strain rate not exceeding 50% per minute shall not be less than the following: - Yield Strength: 12,000 psi - Elongation at yield: 3% - Longitudinal Tensile strength: 22,000 psi - Traverse Tensile strength: 25,000 psi - Longitudinal Elongation at break: 90% - Traverse Elongation at break: 75% In most cases, a 7 mil retention film will be sufficient to meet the minimum physical properties.	50

Security Criterion	Detail	Criteria Page
Blast Resistance – Façade and Structure	Reference the current DBT established by the ISC, unless device size is superseded by an agency-specific threat assessment. Device location is the closest possible point to the protected setback with the DBT device. All building materials and types acceptable under model building codes are allowed. Design detailing is required for material such as pre-stressed concrete, pre-cast concrete, and masonry to adequately respond to the design loads. Unreinforced masonry is unacceptable. Pre-stressed concrete is not very ductile and may not be appropriate where load reversals may occur. The construction type selected must meet all performance criteria for the specified Protection Level. All building components requiring blast resistance must be designed using established methods and approaches for determining dynamic loads, structural detailing, and dynamic structural response. The demands on the structure will be equal to the combined effects of dead, live, and blast loads. Blast loads or dynamic rebound may occur in directions opposed to typical gravity loads. Design and analysis approaches should be consistent with U.S. Department of the Army Technical Manuals. Response limits shall follow U.S. Army Corps of Engineers PDC-TR 06-08, “Single Degree of Freedom Structural Response Limits for Antiterrorism Design." Medium Façade Protection: Moderate damage, repairable. The facility will sustain a significant degree of damage, but the structure should be reusable. Assets may be damaged. Building elements other than major structural members may require replacement. High Façade Protection: Minor damage, repairable. The facility or protected space may globally sustain minor damage with some local significant damage possible. Assets may receive minor damage. For new construction projects and major rehabilitation projects over 100,000 GSF, a blast engineer with formal training in structural dynamics, and demonstrated experience with accepted design practices for blast resistant design must be included as a member of the design team.	50

Security Criterion	Detail	Criteria Page
Blast Resistance - Progressive Collapse	Reference the current DBT established by the ISC, unless device size is superseded by an agency-specific threat assessment. Device location is the closest possible point to the protected setback with the DBT device. Analysis for progressive collapse shall follow GSA's Progressive Collapse Analysis and Design Guidelines for New Federal Office Buildings and Major Modernization Projects, dated June 2003 with the addendum that buildings of three stories or less above grade are exempt from progressive collapse consideration. All building materials and types acceptable under model building codes are allowed. Careful detailing is required for material such as pre-stressed concrete, pre-cast concrete, and masonry to adequately respond to the design loads. Unreinforced masonry is unacceptable. Pre-stressed concrete is not very ductile and may not be appropriate where load reversals may occur. The construction type selected must meet all performance criteria for the specified Protection Level. For new construction projects and major rehabilitation projects over 100,000 GSF, a blast engineer with formal training in structural dynamics, and demonstrated experience with accepted design practices for blast resistant design must be included as a member of the design team. Designers may apply static and/or dynamic methods of analysis to meet this requirement. Ultimate load capacities may be assumed in the analyses.	50
Blast Resistance - Under-Building Parking	Reference the current DBT established by the ISC, unless device size is superseded by an agency-specific threat assessment. Device location is the closest possible point to columns supporting the facility structure above, taking into account other protective measures to prevent access with the DBT device. The use of vehicle screening before vehicles are allowed to enter the parking garage can force adversaries to reduce device size and limit it to the amount that can be concealed from screening. Different screening measures are more effective: visual inspections of passenger areas and trunks may detect large quantities, but smaller quantities can still be hidden inside door panels and under seats. Trace detection systems and K-9 teams can identify very small quantities.	50
Burglary Resistance of Windows	Forced entry resistance should be uniform around the perimeter and the façade of the building. Utilize a balanced approach to the installation of windows which resist forced entry comparable to the windows and doors of the facility and secure areas. The degree of penetration resistance should be commensurate with the delay necessary to protect assets while security and law enforcement personnel are notified and respond. Additional information is available in State Department Standard DOS SD-STD-01.01, Revision G, Certification Standard - Forced Entry and Ballistic Resistance of Structural Systems. Additional solutions may include burglary-resistant bars, wire mesh window systems, etc.	50

Security Criterion	Detail	Criteria Page
Walls and Nonwindow Openings	Forced entry resistance should be uniform around the perimeter and the façade of the building. Utilize a balanced approach to the installation of windows which resist forced entry comparable to the windows and doors of the facility and secure areas. The degree of penetration resistance should be commensurate with the delay necessary to protect assets while security and law enforcement personnel are notified and respond. Additional information is available in State Department Standard DOS SD-STD-01.01, Revision G, Certification Standard - Forced Entry and Ballistic Resistance of Structural Systems. Additional solutions may include burglary-resistant bars, wire mesh window systems, etc. Nonwindow openings greater than 96 square inches in perimeter walls should be secured with grilles, bars, or alarms.	52
Windows in Critical Areas - Ballistic Protection	Reference the current DBT established by the ISC, unless caliber and/or weapon type is superseded by an agency-specific threat assessment. The tenant agency should determine which offices meet the threshold of "critical" based on the occupant.	52
Protection of Air Intakes	Securing air intakes makes the building ventilation system less accessible and therefore less vulnerable to threats that might introduce contaminates directly into the intakes. When choosing secure locations for intakes in urban areas, take into consideration the vantage points offered to threats from nearby buildings and roofs. Additional information is available in The Centers for Disease Control and Prevention Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks.	52
Isolated Ventilation Systems	In addition to the systems being separate from the rest of the facility, HVAC systems serving lobbies, mailrooms, and loading docks shall not share a return-air system with each other. The areas served by a dedicated exhaust system shall be maintained at a negative pressure relative to the rest of the building, but at a positive pressure relative to the outdoors. Physical isolation of these areas (well-sealed floor to roof-deck walls, sealed wall penetrations) is critical to maintaining the pressure differential and requires special attention to ensure airtight boundaries between these areas and adjacent spaces.	52
HVAC Control	Written shut-down procedures shall be included as part of the facility's security and occupant emergency plans. A "one-step shut-off" is a mechanism that requires only a single action by an individual (e.g., engineer or security personnel) to initiate the immediate shut down of all air handling equipment in the building. One-step shut-off controls referenced at Level IV and V must be immediately accessible to authorized personnel at all times, such as in a security control center, staffed engineering office, or other location staffed at all times the facility is occupied. Special air-filtration systems designed to continue to operate in a contaminated environment to enable mission continuity are acceptable.	52

Security Criterion	Detail	Criteria Page
CBR Detection Technology	Reference the current DBT established by the ISC, unless CBR threat type is superseded by an agency-specific threat assessment. Detectors may be located inside HVAC systems, within critical areas or locations susceptible to CBR release, or outside the building on the site. Detectors should provide sufficient advanced warning to allow emergency shutdown, evacuation, and/or shelter-in-place actions to be implemented.	52
Biological Filtration - General Building	Additional information is available in the U.S. Army Corps of Engineers ETL 1110-3-498, "Design of Collective Protection Shelters to Resist Chemical, Biological, and Radiological (CBR) Agents."	54
Biological Filtration - Lobbies and Mailrooms	Additional information is available in the U.S. Army Corps of Engineers ETL 1110-3-498, "Design of Collective Protection Shelters to Resist Chemical, Biological, and Radiological (CBR) Agents."	54
Chemical Filtration	Reference the current DBT established by the ISC, unless CBR threat type is superseded by an agency-specific threat assessment. There are a variety of gas adsorption filter medias available. Each is designed for a particular application (e.g., trace acids, alkalines, VOCs, etc.). It is unlikely that any of these filter medias is 100% efficient. The efficiency rate will vary based on many factors, such as contaminant concentration, how the filters are sealed in the housing, length of contaminant challenge, service life of filters, etc. In summary, these systems are costly, must be specific for intended application, and are somewhat limited in their effectiveness.	54
Security of Ventilation Equipment and Controls	In order to ensure HVAC system operation cannot be disrupted by someone physically accessing the controls, HVAC equipment should be located in a secure area with access limited to security and engineering staff.	54
Location of Utilities and Feeders	Reference the current DBT established by the ISC, unless device size is superseded by an agency-specific threat assessment. Underground service is preferred, and any access points should be controlled. If utility systems cannot be located away from high-risk areas, service feeds, equipment, or equipment rooms should be hardened.	54
Separation of Emergency and Normal Power Distribution	Emergency power may not be available in small buildings except for a UPS system.	54
Emergency Generator Protection	Reference the current DBT established by the ISC, unless device size is superseded by an agency-specific threat assessment. Emergency generators may be required to support the tenant mission, life-safety requirements, or as part of the uninterruptable power supply for security systems. More secure locations include the roof, protected grade level, and protected interior areas. If the emergency generator is installed outdoors at grade, it should be protected by perimeter walls and locked entrances. The generator should not be located in any areas that are prone to flooding. Provisions for securing refueling and shut-off valves in fuel lines within or in close proximity to the building must be addressed.	54

Security Criterion	Detail	Criteria Page
Protection of Water Supply	Reference the current DBT established by the ISC, unless CBR threat type is superseded by an agency-specific threat assessment.	54

Facility Entrances

Security Criterion	Detail	Criteria Page
Badge Identification (ID) System	A photo ID must be worn on the person so that it is visible from the front, waist level or higher. The picture on the ID should be updated regularly. Other applicable regulations may apply (e.g., HSPD-12).	56
Regulatory Signage	Examples of appropriate signage include but are not limited to: - Prohibiting the unauthorized possession of firearms and dangerous weapons - Consent to search - Local building rules and regulations regarding prohibited items - CCTV surveillance advisory - Federal property/No Trespassing signs Refer to 41 CFR 102-74 for further examples.	56
Employee Access Control	At a minimum, the guard must be able to compare the employee's face to the photo on the ID. It is preferable that the guard physically touch the ID badge as a further measure to detect counterfeiting.	56
Visitor Access Control	Personnel escorting visitors must maintain a visual line of sight, physical proximity, or other means of control of the visitor(s). The ratio of visitors to escorts shall be established by the FSC or agency security organization based on operational requirements. Visitors may require vetting prior to granting access to confirm identity and security clearances as needed. Approval for unescorted access will be based on a facility access policy set by the FSC or Designated Official.	56
Occupant Screening	Generally, screening is accomplished using non-intrusive electronic methods such as X-rays and magnetometers, but also may include hand-searches, visual searches, chemical swabs, hand-wands, or other means. Established procedures for initial and follow-up screening must be followed, and screening personnel must be appropriately trained in the procedures and operation of all screening equipment. Screening equipment should be calibrated according to manufacturer's specifications on a regular basis (preferably daily).	56
Visitor Screening	Generally, screening is accomplished using non-intrusive electronic methods such as x-rays and magnetometers, but may also include hand-searches, visual searches, chemical swabs, hand-wands, or other means. Established procedures for initial and follow-up screening must be followed, and screening personnel must be appropriately trained in the procedures and operation of all screening equipment. Screening equipment should be calibrated according to manufacturers' specifications on a regular basis (preferably daily). Exceptions to visitor screening may be implemented to accommodate Law Enforcement Officials, VIP's (e.g., the President, Agency Head) and other such individuals as determined by the DO and the FSC.	56
Ballistic Protection at Screening Locations	Follow DBT weapon requirements and Underwriters Laboratory (UL) 752 Ballistic Standards.	56

Security Criterion	Detail	Criteria Page
Lobby Queuing	Having a substantial number of unscreened personnel outside the secure area awaiting entry can present a target of opportunity to adversaries. Queuing is reduced by increasing throughput, while maintaining the effectives of the security measures. Increasing the number of visitor receptionists, the number of screening lanes, and the processing speed of access control systems can all reduce queuing time. In order to prevent incidents in the lobby from impacting the rest of the facility, designing a "sacrificial lobby" or stand-alone visitor screening area outside the main building foot-print is allowed. The boundaries between the lobby and the remainder of the facility must be constructed to protect the building from the air blast occurring on the unsecured side of the lobby.	56
After Hours Access Control	The building register should document at least the name, purpose, date, time in and out, and a point of contact for visitors. Use of an electronic access control system utilizing read-on-exit would constitute an electronic sign out.	58
Limit Building Entry Points	All building entry points must be controlled and/or monitored. Reducing the number of building entry points, particularly under periods of heightened threat, reduces vulnerability and security costs associated with monitoring and controlling access.	58
Entrance Co-location	Separating employee and visitor entrances improves employee throughput and allows for more efficient screening of visitors. Additionally, where the risk of violence perpetrated by a visitor on an employee exists, separating the flow patterns may reduce this risk.	58
Perimeter Doors & Door Locks	Forced entry resistance should be uniform around the perimeter and the façade of the building. Utilize a balanced approach to the installation of doors which resist forced entry comparable to the windows and walls of the facility. The degree of penetration resistance should be commensurate with the delay necessary to protect assets while security and law enforcement personnel are notified and respond. Additional information is available in State Department Standard DOS SD-STD-01.01, Revision G, Certification Standard - Forced Entry and Ballistic Resistance of Structural Systems. Hinge pins located on the unsecured side of perimeter and critical interior doors must be designed to preclude door removal. Magnetic locks should have at least 1,200 pounds of shear holding power. Electric strikes should meet all specification of UL Standard 1034, Burglary-Resistant Electric Locking Mechanisms. For information on high-security locks, refer to Underwriters Laboratory (UL) Standard 437, Key Locks, American National Standards Institute (ANSI) Standard A156.30-2003, American National Standard for High Security Cylinders, and ANSI Standard 156.5-2001, American National Standard for Auxiliary Locks and Associated Products.	58
Control of Keys and Access Media	Access media may include card keys, electronic keys, biometric devices, etc. All keys and access media should be tracked and inventoried on a regular basis. When an employee no longer requires access, all keys and access media must be recovered or disabled. When keys or access media are reported lost or stolen, they must be deactivated and/or locks should be changed.	58

Security Criterion	Detail	Criteria Page
Employee Convenience Doors	The use of unguarded employee convenience doors is discouraged. If used, they should be in locations where they can be monitored, and checked during routine roving guard patrols. Physical (electronic) access control systems using multifactor authentication technology are recommended for all unguarded entry doors. Such entry doors also should be under CCTV camera coverage, with video recording. Anti-pass back and anti-tailgating at unguarded doors should be addressed through training and electronic-system programming.	58
Emergency Exit Doors	Electronic locks on perimeter doors must fail-secure, and electronic locks on interior doors must fail-safe, if such measures do not conflict with applicable fire and safety codes.	58
Delayed Egress	Delayed egress doors should be used in areas where egress would need to be delayed until security forces can respond and/or CCTV coverage can adequately record the event. Delayed egress should be used for such applications as child-care centers, where children must be prevented from leaving the area unescorted, or from money transaction areas.	58

Interior

Security Criterion	Detail	Criteria Page
Space Planning	Critical systems and equipment may include security and life-safety systems, power distribution, communications and data, and other mission-critical equipment.	60
Access to Nonpublic Areas	The level of protection afforded by the boundaries should be commensurate with the risk to each nonpublic area. A single facility may have nonpublic areas protected at various LOPs.	60
Security of Critical Areas	Critical areas include communications rooms, data centers, operations, and command centers, etc. The following source documents provide Federal physical security requirements for various critical and sensitive areas within facilities. These national requirements are normally augmented by additional agency or departmental specific requirements. SCIFS: Director Central Intelligence Directive (DCID) 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities. Non-classified IT Systems: NIST Special Publication 800-53, Revision 2, December 2007, Appendix F-PE. Classified IT Systems: DCID 6/3, DCID 6/9, and DCID 6/4. Open Storage Areas: National Archives and Records Administration's Information Security Oversight Office (ISOO) Directive 1, parts 2001.43 and 2001.52. Additional security measures may be found in the Department of Defense National Industrial Security Program Operating Manual (NISPOM), issued February 28, 2006, Chapter 5. COMSEC Facilities: National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4005, Safeguarding Communications Security (COMSEC) Facilities and Materials dated August 1997, as amended by NSTISSC [Memorandum] 003-98 and Committee on National Security Systems (CNSS) [Memorandum] CNSS-079-03, dated 5 August 2003. Special Access Program Facilities: Joint Air Force, Army, Navy (JAFAN 6/9) Manual: Physical Security Standards For Special Access Program Facilities, 23 March 2004.	60
Building Systems and Roof Access	Hinge pins located on the unsecured side of perimeter and critical interior doors must be designed to preclude door removal. Magnetic locks should have at least 1,200 pounds of shear holding power. Electric strikes should meet all specification of Underwriters Laboratory (UL) Standard 1034, Burglary-Resistant Electric Locking Mechanisms. For information on high-security locks, refer to UL Standard 437, Key Locks, American National Standards Institute (ANSI) Standard A156.30-2003, American National Standard for High Security Cylinders, and ANSI Standard 156.5-2001, American National Standard for Auxiliary Locks and Associated Products. Where roof access allows entry to critical building or air intakes, CCTV monitoring and recording should be used in conjunction with locking and detection devices.	60
Publicly Accessible Restrooms	When public access to restrooms is allowed, the level of protection afforded by the boundaries with nonpublic areas should be commensurate with the risk to each nonpublic area. See Access to Nonpublic Areas.	60

Security Criterion	Detail	Criteria Page
Publicly Accessible Retail and Mixed Use Space	While important to the public nature of buildings, the presence of retail and other mixed uses may present a risk to the building and its occupants, and should be carefully considered on a project-specific basis during the risk-assessment process.	60
Blast Resistance - Interior Public Spaces	Reference the current DBT document. Explosive device location for design purposes is the closest possible point to accessible columns, critical utilities, etc. Take into account other protective measures to prevent access with the DBT device, such as screening prior to entry.	60
Blast Resistance - Mail Screening and Receiving Location	Reference the current DBT document. Explosive device location for design purposes is the area where mail is screened, sorted, or staged awaiting screening. Instruct personnel not to leave unscreened mail next to columns surrounding the mail screening and receiving area or against walls abutting critical areas. Off-site mail screening facilities are in essence a measure of preventing progressive collapse and limiting air blast from the DBT at the facilities they serve.	62
Interior Windows	No special measures required if the DBT device for VBIEDs and hand-carried external events (see DBT document) would not create pressures greater than 1 psi on interior windows (due to setback and other protective measures).	62

Security Systems

Security Criterion	Detail	Criteria Page
CCTV Coverage	The design of the system will vary depending on the objective of the surveillance, environment, facility type, and end-user requirements. Use of a professional for the design and installation is essential to maximize the operational effectiveness of CCTV systems and integration with other physical security equipment. Considerations for CCTV coverage include: - Image quality in all lighting conditions - Lens selection for area versus detail coverage and resolution - Color versus black-and-white images - Fixed cameras dedicated to monitoring specific locations full-time versus pan-tilt-zoom cameras which can be used for active investigation of activity - Blind spots	64
CCTV Monitoring and Recording	Certain facilities or CCTV views should be actively monitored (including using alarm-integrated CCTV cameras) to facilitate real-time detection and investigation of an incident, and to coordinate an active response to an incident. Other facilities or views may be recorded for forensic purposes only. Security personnel assigned to actively monitor CCTV should be relieved regularly and only be tasked to monitor a limited number of camera views to alleviate fatigue and inattentiveness. Security officials should determine the length of time that personnel can effectively monitor cameras based on the number of views and other activities. An option to minimize fatigue and maximize coverage is the use of sequencing and multiplexing of multiple camera views on the same screen. CCTV recording is intended to develop and maintain a video log of activities which may be referenced if an event is noted after the fact. Each agency should determine the length of time for which digital images should be stored, based on facility operations and equipment capabilities. Security officials should establish protocols to minimize and control access to the CCTV operating system and stored images. Considerations for CCTV monitoring and recording include: - If the CCTV data is to be transmitted on an IT LAN, determine if the LAN has the capability of providing the minimum level of video resolution, frame rate, and system reliability to satisfy physical security protection needs. - How much and what type of data needs to be retrieved from the system for evidence. CCTV systems may record continuously or only as required to monitor a particular event such as an alarm. - A chain of custody for evidence retrieval (contact isfubgroup@tswg.gov for a publication on Best Practices for the Retrieval of Video Evidence from Digital CCTV Systems or visit www.tswg.gov.) - The need for disaster recovery and remote operational capability, including off-site storage of data	64

Security Criterion	Detail	Criteria Page
Security Control Center	The Security Control Center should incorporate the following (if provided at the facility): - IDS monitoring - CCTV monitoring - Communications equipment for the guard force - Access control system controls - Fire and other emergency alarm annunciation - HVAC emergency shut-off - Building emergency communications system - Sufficient phone hard lines for incoming and outgoing calls during an incident. These lines may be recorded. - Secure storage of all building plans, security equipment circuit runs, guard post orders, OEP, COOP, and emergency contacts for security equipment manufacturers. - External emergency notification equipment deemed necessary by the security provider The security control center should be secured as a critical area, and access should be limited to security personnel.	64
CCTV Surveillance Advisory	Signs should be posted at entrances to the site, facility, parking garages, etc., where CCTV coverage exists.	64

Security Criterion	Detail	Criteria Page
Intrusion Detection System (IDS) Coverage	There are three major groupings of Intrusion Detection Systems (IDS). The following descriptions are provided as benchmarks in considering the appropriate system technologies. All three types are generally used in conjunction with an access control system. 1. Basic Security-in-Depth IDS—Entry Doors: magnetic switch, alarm system keypad, passive infrared sensor (PIR), and an alarm panel (to designated monitoring center). Windows and other openings: glass-break detector, magnetic switches or shock sensors. (Low to Medium LOP) 2. High Security-in Depth IDS—Entry Doors: Balanced magnetic switch (BMS) or High Security Switch (HSS – UL634 Level 2), PIR, alarm system keypad, alarm system panel (UL1076), with all devices having an individual tamper sensor. Windows (if present) and other openings: glass-break detector, balanced magnetic switches, or shock sensors. IDS control panel fully integrated with other security measures, for example, CCTV cameras, other security systems (lockdown), sound, heat, and vibration/impact sensors located in critical area(s) or throughout the facility as necessary; also integrated with fire safety system. (SCIFs, open storage areas for collateral classified information, and high consequence lab space, require a high security IDS.) (High LOP) 3. Very High Security-in-Depth IDS—Security Management System: high security IDS system encompassing detection and alarm devices positioned at the site perimeter, restricted areas between the site perimeter and the building, building entrances, and rooms and/or areas within the facility (Very High LOP). In a facility requiring a Very High LOP that has no external perimeter, hardening of the first floor may be necessary which may encompass minimizing all entry points, alarming all entry points, enclosing window spaces, and alarming interior rooms and spaces on the first floor with motion detector (volumetric sensors). The technologies used in IDS systems range from relatively basic electrical contact mechanisms (magnetic switch), keypads, and alarm panels connected to a monitoring center to high security devices such as balanced magnetic switches, tamper sensors, motion, heat, sound, or vibration sensors, and other devices that are fully integrated. The specific technologies used should be based on a threat/risk management assessment considering criticality, consequences, and cost. Professional design, engineering, and installation are critical to ensure operational effectiveness of the IDS system itself and its integration with other physical security equipment. UL Listed intrusion detection equipment is strongly recommended. Initial installation should include validation [testing] of the entire system, including monitoring center notification and connected equipment. Periodic testing and maintenance are required to ensure continuous operational effectiveness. Schedule and record results accordingly. Repair/replace malfunctioning equipment as needed based on testing and maintenance results.	64
Intrusion Detection System (IDS) Monitoring	IDS at certain facilities or protected areas should be actively monitored to facilitate a real-time detection of an incident, and to coordinate an active response to an incident. IDS should be integrated with CCTV systems to the greatest extent possible to facilitate immediate alarm assessment. IDS activity logs are intended to develop and maintain a record of alarm activities which may be referenced if an event is noted after the fact. Each agency should determine the length of time for which alarm activity records should be stored, based on facility operations and equipment capabilities.	64

Security Criterion	Detail	Criteria Page
Duress Alarms or Assistance Stations	Duress alarms should be used at areas such as guard stations, interview rooms, cash/public transaction areas, or at-risk areas. Duress devices shall be concealed from the public and shall annunciate for an immediate response. Duress buttons on guard radios are acceptable for duress buttons at guard posts. Procedures on response and telephone contact where the alarm occurred shall be established.	64
Security System Integrity	In addition to controlling physical access, logical access for programming and recordkeeping must be limited to personnel with administrative rights as necessary to maintain and program the system. Computer-based systems also may be required to meet agency-specific CIO certification and accreditation requirements.	64
Security Communications	For larger or busier guard forces, it may be necessary to designate a "dispatcher" to control the radio network. Consideration should be given to digitally recording guard force communications. The radio network should be designed to ensure adequate coverage throughout the facility, and enable a user to contact a communications center regarding tasks, reporting incidents, and requesting assistance.	64
Building Communication System	The building communication system should be utilized to provide emergency announcements, alerts, and instructions to occupants. On-site communication with guards, designated response personnel and OEP support employees is essential during an incident. Procedures for standard announcements and drills shall be developed. Standard announcements could be prerecorded into the building communication system for immediate notification by the security provider when warranted. Agencies should identify any hearing impaired occupants and establish alternative procedures to be used in the event of an alert or announcements. Communication may be achieved through public address systems, specially designed phone systems, and computer-based mass delivery.	64
Emergency Power for Security Systems	Uninterruptable power can be provided through the use of batteries, emergency generators, UPS, or a combination thereof to meet the requirements. More than 4 hours of backup may be required for certain facilities based on mission, such as when the facility is required to maintain 24-hour operations.	66
Security System Testing	Testing must be based on established, consistent agency-specific protocols, and documented. Components which fail during testing should be serviced in accordance with the Security System Maintenance criteria.	66

Security Criterion	Detail	Criteria Page
Security System Maintenance	Critical components are those required to provide security (IDS, CCTV, access control, etc.) for a perimeter access point or critical area. "Replacement" may include implementing another temporary measure in instances where the replacement or repair is not achievable within the specified time frame (e.g., a guard to control access or monitor a critical area normally covered by a camera, or a temporary barrier to replace an inoperable pop-up vehicle barrier).	66

Operations and Administration

Security Criterion	Detail	Criteria Page
Designated Official (DO)	The DO will comply with the ISC's "Facility Security Committees" standard.	68
Facility Security Committee (FSC)	The FSC will comply with the ISC's "Facility Security Committees" standard. In single-tenant facilities, establishment of a formal FSC is optional.	68
Security Operations Management	In cases where the security organization does not have a presence at the facility or in the region sufficient to meet these requirements, the DO and FSC will designate an on-site employee to serve in this capacity. If the facility has a guard force, the contracting agency will designate (at the request of the DO/FSC) an on-site employee to serve as a COTR, with the authority to reassign and direct guard operations during emergencies. The on-site security manager's duties include, but are not limited to: - Contract guard coordination and oversight; - Security equipment testing and maintenance; - Review security assessments and current intelligence information; - Guard post order development and update; - Ensure implementation of building-specific security policies; - Coordinate with the responsible facility owner (e.g., GSA or lessor) the installation, maintenance, testing, repair, and replacement of security equipment; - Maintaining close liaison with the DO, FSC, and local first responders; and, - The authority to direct guard force deployment in emergency situations. Security personnel should receive recurring training on current principles, practices, and trends in technology.	68
Guard Fixed Post - Exterior	Require guards to request the presentation of a government issued ID (e.g., driver's license or other photo ID) from persons for visual and physical inspection prior to entering the building.	68
Guard Fixed Posts - Screening Checkpoints	Screening checkpoint staffing shall be based on the principle that one guard only performs one screening task at a time. Consideration must be given to throughput and checkpoint configuration in making this determination.	68
Guard Patrols	Patrols should be random in nature so as not to establish a predictable pattern that can be circumvented by an adversary. However, the frequency with which a patrol passes any given point on the patrol route should be not more than 1 hour.	68
Guard Response	For facilities that do not have a dedicated security team available for incident response, rovers may be used or posts may temporarily be shut down to provide personnel for a response to an incident. Established procedures and post orders should outline these situations.	68

Security Criterion	Detail	Criteria Page
Facility Security Plan	The Facility Security Plan provides direction to security personnel on the security management and policies of the building. At a minimum, the Facility Security Plan should: - Identify security related responsibilities; - Identify current and planned security measures; - Define building-specific security policies; - Contain emergency contacts (such as law enforcement, first responders, security organization, and facility manager); - Detail response procedures for emergencies; - Outline approved protocols for access by employees, contractors, and visitors; - Establish changes in security operations due to temporary upgrades in the homeland security advisory system; and, - Outline the security measure testing schedule performed by the security manager at level IV and V facilities; and, - Identify security support requirements for the OEP. The level of detail to which the plan is written may vary based on the nature of the facility (e.g., Level I facilities may have very abbreviated documents). The plan should be protected as FOUO at minimum.	68
Occupant Emergency Plan (OEP)	The OEP provides direction to the occupants of the building on how to react to emergencies. At a minimum, the OEP should address: - Purpose and circumstances for activation; - Command officials and supporting personnel contact information; - Occupant life-safety options (evacuation, shelter-in-place); - Local law enforcement and first responder response; - Special needs individuals (disabled, deaf, etc.); - Visitors; - Special facilities (e.g., SCIFs, child-care centers); - Assembly and accountability; - Security during and after incident; and, - Training and exercises. The scope and complexity of the OEP is dependent on the facility's size, population, and mission. The OEP must be reviewed annually and updated as appropriate. OEPs must also identify unique planning requirements for staff or functions such as evacuating child-care centers.	68
Availability of Emergency Plans and Documents	The DO and other emergency management personnel should have immediate access to the OEP, emergency instructions, building plans, the Facility Security Plan, and contact and communication information. Access to these plans after hours also should be ensured.	68

Security Criterion	Detail	Criteria Page
Protection of Construction Information	The availability of information on construction, including Web-cam views, must be limited to those with a need-to-know in order to hinder pre-operational planning by adversaries. All efforts should be made to disrupt the planning cycle and increase the chances of discovering a hostile intelligence-gathering operation. The greatest chance of discovery comes when the adversary has to come on or near the site to gather information. If Web-cameras (or similar technology) are used to broadcast construction progress, or construction documents are online, access must be encrypted and password-protected.	68
Security During Construction and Renovation	A Construction Security Plan should describe how the government's assets, information, equipment, and personnel are protected during the construction process. Construction projects range from small interior space alterations, to building additions, to the construction of a new facility or complex. Required security measures should vary accordingly commensurate with associated threats, vulnerabilities, and consequences. The plan should specify who is responsible for the security of the site during each phase of the project until final completion to include access to the construction site or area within an existing building, and those areas requiring access in order to reach the actual construction area. Security needs may increase or decrease as the project progresses from initial start (demolition or groundbreaking) through substantial completion, that is, when the government assumes control of the facility and progressive occupancy begins. Critical areas within, or adjacent to, the project may require special, more stringent security measures to protect government assets and information. In developing the construction security plan, the security professional should assess all reasonable threats and vulnerabilities to government assets, information, equipment, and people. Elements to consider in developing a Construction Security Plan include, but are not limited to, the following: • Perimeter security (site, clear zones, restricted access to areas within a building, etc.) • Security of construction trailer/construction office • Access control (background checks, clearances, alien status, etc.) • Badging (construction worker ID badges and processing; escort/no escort required; lost badge procedures; access termination procedures) • Vehicular access (construction worker parking; construction material deliveries) • Video surveillance (guard posts, critical areas, access points within buildings) • Internal security (key control, sensitive areas, internal theft of government or employee property) • Construction worker movement to or through areas that are still occupied or operational • Security of construction plans: (hard copy and electronic) • Physical barriers; construction area warning signs. • Maintaining security during HAZMAT, law enforcement, fire or medical emergency response Security inspections, such as a Technical Surveillance Countermeasures (TSCM) or explosive detection canine sweep, may be required upon completion of construction work in critical secure areas.	68

Security Criterion	Detail	Criteria Page
Mail/Package Handling and Other Deliveries	Screening should be accomplished by personnel trained in the ISC Best Practices for Safe Mail Handling and in the operation of the screening equipment. Mail screening may be accomplished by security guards or mailroom staff. For mailroom security measures and mitigation of design events, reference GSA's "Guidelines for Mailroom Construction and Renovation" and the U.S. Postal Inspection Service's "Mail Center Security Guide" Publication 166, September 2002 (at www.usps.com).	70
Security Awareness Training	Topics may include: - Security policies and procedures; - Workplace violence; - General crime prevention measures; - Suspicious packages; - Reporting security incidents; - Proper reporting and response to fires and other emergencies; and, - Operational security measures. Other training unique to the mission may be applicable and should be requested by the DO/FSC and provided by the security organization as necessary.	70

This Page Intentionally Left Blank

Appendix B –Acronyms and Definitions

ANSI	American National Standards Institute
ASTM	American Society for Testing and Materials
BSC	Building Security Committee
CBR	Chemical-Biological-Radiological
CCC	Child-Care Center
CCTV	Closed-Circuit Television
CDC	Centers for Disease Control and Prevention
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CPTED	Crime Prevention Through Environmental Design
DBT	Design-Basis Threat
DHS	Department of Homeland Security
DO	Designated Official
FOUO	For Official Use Only
FSC	Facility Security Committee
FSL	Facility Security Level
GSA	General Services Administration
IDS	Intrusion-Detection System
IES	Illuminating Engineering Society
ISC	Interagency Security Committee
LOP	Level of Protection
NRC	Nuclear Regulatory Commission
UL	Underwriters Laboratory
USC	United States Code
VBIED	Vehicle-Borne Improvised Explosive Device
WMD	Weapons of Mass Destruction

Adjacency: A building or other improvement that abuts or is proximate to a multiple building site, a specific building within a multiple building site, or a single building site.

Alteration: A limited construction project for an existing building that comprises the modification or replacement of one or a number of existing building systems or components. An alteration goes beyond normal maintenance activities but is less extensive than a major modernization.

Baseline LOP: The degree of security provided by the set of countermeasures identified in this document for each FSL which must be implemented unless a deviation (up or down) is justified by a risk assessment.

Building: An enclosed structure (above or below grade).

Building Entry: An access point into, or exit from, the building.

Building Envelope: The outside surface and dimensions of a building, inclusive of the façade and roof.

Campus: Two or more Federal facilities located on one site and typically sharing some aspects of the environment, such as parking, courtyards, private vehicle access roads, or gates and entrances to connected buildings. A campus also may be referred to as a "Federal center" or "complex."

Consequence: The level, duration, and nature of the loss resulting from an undesirable event.

Critical Areas: Areas that if damaged and/or compromised could have significant adverse consequences for the agency's mission or the health and safety of individuals within the building or the surrounding community. Also may be referred to as "limited access areas," "restricted areas," or "exclusionary zones." Critical areas do not necessarily have to be within Government-controlled space (e.g., generators located outside Government-controlled space).

Customized LOP: The final set of countermeasures developed as the result of the risk-based analytical process.

Designated Official (DO): The highest ranking official of the primary tenant agency of a Federal facility or, alternatively, a designee selected by mutual agreement of tenant agency officials.

Design-Basis Threat (DBT): A profile of the type, composition, and capabilities of an adversary.

Existing Federal Facility: A facility that has already been constructed or for which the design and construction effort has reached a stage where design changes may be cost prohibitive.

Existing LOP: The degree of security provided by the set of countermeasures determined to be in existence at a facility.

Exterior: Area between the building envelope and the site perimeter.

Façade: The exterior face of a building, inclusive of the outer walls and windows.

Facility: Space built or established to serve a particular purpose. The facility is inclusive of a building or suite and associated support infrastructure (e.g., parking or utilities) and land.

Facility Security Committee (FSC): A committee responsible for addressing facility-specific security issues and approving the implementation of security measures and practices. The FSC consists of representatives of all Federal tenants in the facility, the security organization, and the owning or leasing department or agency. In the case of new construction, major modernization, alternation, or lease actions, the FSC will also include the construction or lease procurement project team and the planned tenant(s). The FSC was formerly known as the Building Security Committee (BSC).

Facility Security Level (FSL): A categorization based on the analysis of several security-related facility factors, which serves as the basis for the implementation of physical security measures specified in ISC standards.

Federal Departments and Agencies: Those executive departments enumerated in 5 U.S.C. 101 and DHS, independent establishments as defined by 5 U.S.C. 104(1), Government corporations as defined by 5 U.S.C. 103(1), and the U.S. Postal Service.

Federal Facilities: Leased and owned facilities in the United States (inclusive of its territories) occupied by executive branch Federal employees for nonmilitary activities.

Government-Owned: A facility owned by the United States and under the custody and control of a Federal department or agency.

Interior: Space inside a building controlled or occupied by the Government.

Lease Construction (Build-to-Suit): A new construction project undertaken by a lessor in response to a specific requirement for the construction of a new facility for the government.

Lease Extension: An extension of the expiration date of a lease to provide for continued occupancy on a short-term basis.

Lease Renewal (Exercised Option): The exercising of an option to continue occupancy based upon specified terms and conditions in the current lease agreement.

Level of Protection (LOP): The degree of security provided by a particular countermeasure or set of countermeasures. Levels of protection used in this Standard are Minimum, Low, Moderate, High, and Very High.

Level of Risk: The combined measure of the threat, vulnerability, and consequences posed to a facility from a specified undesirable event.

Major Modernization: The comprehensive replacement or restoration of, or addition to, virtually all major systems, tenant-related interior work (such as ceilings, partitions, doors, floor finishes, etc.), or building elements and features.

Necessary LOP: The degree of security determined to be needed to mitigate the assessed risks at the facility.

New Construction: A project in which an entirely new facility is to be built.

New Lease: A lease established in a new location when space must be added to the current leased space inventory.

Occupant: Any person who is permanently or regularly assigned to the government facility and displays the required identification badge/pass for access. The FSC establishes the thresholds for determining who qualifies for "occupant" status.

Outlease: The practice of an owning Government agency leasing Government space to nongovernmental tenants.

Primary Tenant: The Federal tenant identified by Bureau Code in OMB Circular No. A-11, Appendix C, which occupies the largest amount of rentable space in a Federal facility.

Risk: A measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence.

Risk Acceptance: The explicit or implicit decision not to take an action that would affect all or part of a particular risk

Risk Assessment: The process of evaluating credible threats, identifying vulnerabilities, and assessing consequences.

Risk Assessment Report: The documentation of the risk assessment process to include the identification of undesirable events, consequences, and vulnerabilities and the recommendation of specific security measures commensurate with the level of risk.

Risk Management: A comprehensive approach to allocating resources for the protection of a facility, assets, and occupants to achieve an acceptable level of risk. Risk management decisions are based on the application of risk assessment, risk mitigation, and—when necessary—risk acceptance.

Risk Mitigation: The application of strategies and countermeasures to reduce the threat of, vulnerability to, or consequences from an undesirable event.

Security Organization: The Government agency or an internal agency component responsible for physical security for the specific facility.

Setback: The distance from the façade to any point where an unscreened or otherwise unauthorized vehicle can travel or park.

Site: The physical land area controlled by the Government by right of ownership, leasehold interest, permit, or other legal conveyance, upon which a facility is placed.

Site Entry: A vehicle or pedestrian access point into, or exit from, the site.

Site Perimeter: The outermost boundary of a site. The site perimeter is often delineated by the property line.

Special-Use Facilities: An entire facility or space within a facility itself that contains environments, equipment, or data normally not housed in typical office, storage, or public access facilities. Examples of special-use facilities include, but are not limited to, high-security laboratories, hospitals, aircraft and spacecraft hangers, or unique storage facilities designed specifically for such things as chemicals and explosives.

Standoff: Distance between an explosive device and its target.

Succeeding Lease: A lease established when the Government seeks continued occupancy in the same space at the same leased location, whose effective date immediately follows the expiration date of the existing lease.

Suite: One or more contiguous rooms occupied as a unit.

Suite Entry: An access point into, or exit from, the suite.

Suite Perimeter: The outer walls encircling a suite.

Superseding lease: A lease that replaces an existing lease, prior to the scheduled expiration of the existing lease term.

Threat: The intention and capability of an adversary to initiate an undesirable event.

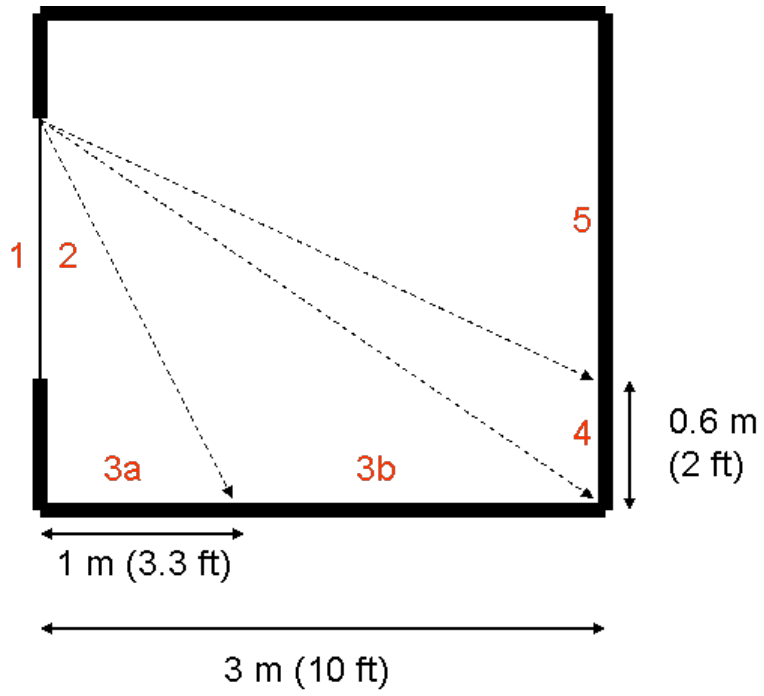
Undesirable Event: An incident that has an adverse impact on the operation of the facility or mission of the agency.

Visitor: Any person entering the government facility who does not possess the required identification badge/pass for access or who otherwise does not qualify as an "occupant."

Vulnerability: A weakness in the design or operation of a facility that an adversary can exploit.

Appendix C – Window Performance Characteristics

Performance Condition	Description of Window Glazing Response
1	Glazing does not break. No visible damage to glazing or frame.
2	Glazing cracks but is retained by the frame. Dusting or very small fragments near sill or on floor acceptable.
3a	Glazing cracks. Fragments enter space and land on floor no further than 1 meter (3.3 feet) from the window.
3b	Glazing cracks. Fragments enter space and land on floor no further than 3 meters (10 feet) from the window.
4	Glazing cracks. Fragments enter space and land on and impact a vertical witness panel at a distance of no more than 3 meters (10 feet) from the window at a height no greater than 0.6 meters (2 feet) above the floor.
5	Glazing cracks and window system fails catastrophically. Fragments enter space impacting a vertical witness panel a distance of no more than 3 meters (10 feet) from the window at a height greater than 0.6 meters (2 feet) above the floor.



For additional information, refer to the U.S. General Services Administration Standard Test Method for Glazing and Window Systems Subject to Dynamic Overpressure Loadings.

This Page Intentionally Left Blank

Appendix D – Sample Risk Acceptance Justification Template

Person Completing Form	Date
Organization	Title
E-mail	Phone

Facility Profile		
Facility Name		Identifier/Bldg #
Address		
City	State	Zip

Facility Security Level		
FSL	Date of FSL	Previous FSL

Factor	Score	Rationale
Mission		
Symbolism		
Population		
Size		
Threat		
Preliminary FSL		
Intangibles		

Risk Assessment Information		
Site Visit Start Date	End	Date of Report
Conducted By		Title
Organization		Phone
E-mail		Cell
Software or Methodology		

Level of Classification/FOUO

Threat Assessment			
Undesirable Event	Baseline Threat (from DBT)	Assessed Threat	Rationale (If Other Than Baseline from DBT)
Aircraft as a Weapon			
Arson			
Assault			
Ballistic Attack			
Ballistic Attack - Small Arms			
Ballistic Attack - Standoff			
Breach of Access Control Point -Covert			
Breach of Access Control Point -Overt			
CBR Release - External Intentional			
CBR Release - Internal Intentional			
CBR Release - Mailed or Delivered			
CBR Release - Water Supply Intentional			
Civil Disturbance			
Coordinated or Sequential Attack			
Disruption of Building & Security Systems			
Explosive Device – Man-Portable External			
Explosive Device – Man-Portable Internal			
Explosive Device - Suicide/Homicide			
Explosive Device – Vehicle Borne IED			
Explosive Device - Mailed or Delivered			
Hostile Surveillance			
Insider Threat			
Kidnapping			
Release of Onsite Hazardous Materials			
Robbery			
Theft			
Unauthorized Entry – Forced			
Unauthorized Entry – Surreptitious			
Vandalism			
Vehicle Ramming			
Workplace Violence			

Level of Classification/FOUO

Risk Acceptance

For each recommendation that will not be fully implemented:

- Summarize the recommendation, including the undesirable event being addressed
- Identify the necessary level of protection that the recommendation would provide
- Summarize any alternative measure being instituted in lieu of the recommended measure
- Identify the LOP the alternative measure will provide
- Provide the justification for why the recommended measure will not be implemented. If applicable, note rationale from choices, and include details as necessary. Use additional paper as necessary to completely describe justification for accepting risk.

Possible Rationales for Risk Acceptance

1. Physical site limitations
2. Facility structural limitations
3. Historical/architectural integrity
4. Building system configuration
5. Adjacent structure impact
6. Funding priorities
7. Short -term occupancy
8. Facility to be excessed
9. Facility to be disposed (provide date)
10. End of lease (provide date)

No signature constitutes acceptance of risk. No rationale constitutes acceptance of risk.

Recommendation	Necessary LOP	Alternative Measure	Achievable LOP	Rationale	DO Signature

Level of Classification/FOUO

This Page Intentionally Left Blank

Interagency Security Committee Participants

ISC Chair

Todd Keil
Assistant Secretary for Infrastructure Protection
U.S. Department of Homeland Security

ISC Executive Director

Austin L. Smith
Interagency Security Committee
Office of Infrastructure Protection
U.S. Department of Homeland Security

Working Group Chair

Everette R. Hilliard
Assistant Director
Justice Protective Service
Security and Emergency Planning
U.S. Department of Justice

Working Group Members

Calvin O. Byrd
Senior Level Advisor for Physical Security
Division of Facilities and Security
Office of Administration
U.S. Nuclear Regulatory Commission

Joseph I. Gerber
Physical Security Specialist
Office of the Chief Security Officer
U.S. Department of Homeland Security

Gwainevere C. Hess
Senior Policy Analyst
Interagency Security Committee
Office of Infrastructure Protection
U.S. Department of Homeland Security

William T. Hirano
Structural Engineer
Engineering and Project Delivery Resources Division
Office of Design & Construction
Public Buildings Service
U.S. General Services Administration

Mark Strickland
Security Specialist
Court Security Office
Administrative Office of the U.S. Courts

Thomas Wood
Chief
Physical Security Branch
Building Security and Policy Division
Public Buildings Service
U.S. General Services Administration

This document could not have been developed without the generous contribution of the departments and agencies who allowed these working group members to participate in this effort, in some cases for periods up to three years.

Also, special thanks to the Nuclear Regulatory Commission for providing technical writing support, and to the Administrative Office of the United States Courts for the use of meeting facilities and information technology support throughout the project.

During the course of the development of this Standard, a number of sites were visited to validate the criteria and process. Thank you to those ISC member departments and agencies which opened their facilities for this important step in our efforts:

Centers for Medicare and Medicaid Services
Customs and Border Protection
Environmental Protection Agency
Federal Aviation Administration
Federal Judiciary
Federal Protective Service
Food and Drug Administration
General Services Administration
National Weather Service
Securities and Exchange Commission
Social Security Administration
U.S. Marshals Service
Veterans Administration

As would be expected during a three-year project, working group members come and go. The working group would like to recognize the extensive contributions of Dennis Chapas and William Kmetz, both now retired from Government service, who participated from the outset of this project until their retirement. Their experience in multiple branches, departments, and agencies throughout the Government greatly enhanced the cross-cutting nature of this standard.

Finally, during the trip to survey the new Oklahoma City Federal Building, the members of the working group toured the Oklahoma City National Memorial and Museum. We are eternally grateful for the opportunity, and thankful to Kari Watkins, Museum Director, and Kerry Pettingill, Director of the Oklahoma Office of Homeland Security and a responder to the bombing, for the personal experience which brought this effort full circle.

We come here to remember those who were killed, those who survived, and those changed forever. May all who leave here know the impact of violence. May this memorial offer comfort, strength, peace, hope, and serenity.

- Inscription at the Oklahoma City National Memorial

The Survivor Tree, an American Elm, stood across the street from the Alfred P. Murrah Federal Building and suffered the force of the blast on April 19, 1995. The tree was nursed back to health and today overlooks the memorial and serves as a living symbol of resilience in the face of terrorism.

Photo courtesy of the Oklahoma City National Memorial Foundation.